O Guia do Hacker Brasileiro – por Marcos Flávio Araújo Assunção

Prefácio

Esse livro se destina àquelas pessoas que gostam de informática e de aprender cada vez mais. Não importa se ao usuário comum ou o técnico, todos se identificarão muito com a obra. Os assuntos serão apresentados de maneira objetiva e universal. Mostrada em uma linguagem clara mas direta, é como um livro de história. Explica, como, onde e por quê a segurança na informática hoje é um problema tão grande. Ela está em nossa vida quando retiramos dinheiro do caixa eletrônico, fazemos compras pela Internet e até quando tiramos algum documento. Viver sem a Internet hoje é indispensável. Conhecer melhor a rede e os seus perigos é imprescindível. O lado mais obscuro da computação atualmente é a segurança, pois é uma faca de dois gumes. Se você sabe como invadir um sistema, sabe como protegê-lo.

É como uma arma. Você sabe que se atirar irá matar alguém, mas entre saber e fazer existe uma grande diferença. Eu não posso me assegurar que você use o conhecimento contido aqui para se proteger, apenas aconselho-o a fazê-lo. Não existe um sistema operacional ideal para estudar junto a esse livro. O meu interesse é mostrar a segurança como um todo, estudando problemas comuns que englobam os sistemas e apenas pequenas diferenças. Na maioria dos exemplos utilizarei programas em Windows, pois são mais fáceis de se explicar para quem está começando. E todos esses programas possuem similares em outros sistemas. Não têm enrolação como páginas e páginas de códigos fontes e informações inúteis: será uma deliciosa viagem de conhecimento real e verdadeiro, adquirido durante meus mais de 6 anos de aventura pela Net.

Meu nome é Marcos Flávio Araújo Assunção, moro em Lavras, MG e estou me mudando em fevereiro de 2002 para Poços de Caldas, MG. Tenho 20 anos e amo a Internet e computação em geral, sou pesquisador amador na àrea, não fiz e nem penso em fazer ciëncias da computação (vou fazer direito), pretendo melhorar esse "livro" a cada nova versão para que se torne um ótimo guia brasileiro sobre hackers. Meu e-mail é mflavio2k@yahoo.com.br e meu UIN no icq é 27672882. Dúvidas e sugestões, à vontade. Se quiser me ligar, meus telefones são: 35-38220176 (Lavras) ou 35-38612309 (Nepomuceno). Não tenho formação nem fiz cursos na àrea. Sou apenas um interessado em estar sempre aprendendo.

A maioria dos programas mencionados no livro podem ser conseguidos nos sites www.blackcode.com. e ftp.technotronic.com Para os outros é só usar sites de downloads como www.superdownloads.com.br .Ferramentas de busca também servem, tais como *Altavista* (www.altavista.com) ou *Google* (www.google.com). Tente também meu site (www.anti-trojans.cjb.net) . Se quiser tirar textos desse livro, indique meu nome na frente.

Introdução à segurança

1

Definições de segurança

Segurança em informática

Estamos seguros?

A fragilidade dos sistemas informatizados não é nenhuma novidade. A décadas, celebridades como *Robert Morris Jr*, *Capitão Crunch*, *Kevin Poulsen* e *Kevin Mitnick*, esses últimos dois mais recentes, fazem com que as pessoas se preocupem e tenham um medo maior do computador. Esse medo virou pânico em pleno século XXI. Piratas novamente existem, mas sua arma não é mais a espada, é o fax-modem. Graças à essa maravilha do mundo moderno, dados podem navegar por linhas telefônicas, cabos e satélites, diminuindo as distâncias entre os povos e iniciando a nova era digital. Ladrões assaltam bancos confortavelmente no Havaí enquanto desviam o dinheiro para a Suíça. A espionagem industrial é um dos problemas agravados. Ela sempre existiu, mas com a facilidade de acesso à Internet, qualquer pessoa pode conseguir dados confidenciais e vendê-los para concorrentes.

Diariamente, páginas e páginas são tiradas do ar por piratas digitais. Grupos de hackers e crackers brasileiros, como *Prime Suspectz e Inferno.br* (esse último já extinto), junto a outros centenas pelo mundo realizam façanhas extraordinárias, como invadir vários sites da Microsoft, a Nasa, FBI, Interpol e muitos outros. Os grupos brasileiros atualmente são os que mais invadem homepages em todo o mundo, fazendo com que a própria Nasa restrinja acesso ao Brasil em algumas de suas páginas. Mas nem todos são ruins. Existem grupos que se especializam em criar ferramentas e ajudar usuários comuns, como o *UHOL*. Toda essa fama já criou até um novo termo no mundo da segurança: o Backer. Ou seja, Brazilian Hacker (Hacker Brasileiro). Isso demonstra a fragilidade da situação. Respondendo à pergunta do tópico: estamos seguros? Com certeza que não.

Características de um sistema inseguro

A segurança de sistemas existe por um conjunto de fatores. Engana-se quem pensa que somente por utilizar uma plataforma Unix ao invés de Windows está seguro. Ou que é só colocar um anti-vírus e um firewall na sua empresa que está tudo bem. A proporção do problema é bem maior. Geralmente os sistemas mais vulneráveis da rede possuem dois pontos em comum:

Administrador

O ponto chave e essencial para qualquer sistema de computador é o administrador. Ele é responsável por fazer com que tudo corra perfeitamente. Checa os dados, administra usuários, controla servidores, checa logs, tudo todos os dias. Acontece que a grande maioria dos administradores hoje não se preocupa com a segurança como deve. Logo terá problemas com o seu sistema, não importa qual seja. É como se fosse mãe e filho. Se uma mãe alimenta seu filho, cuida dos seus deveres de casa, compra roupas novas, dá brinquedos mas não é capaz de comprar um seguro de vida, ou pior, zela tão pouco pela segurança dele que ao sair de casa deixa as portas ou janelas abertas. Essa não pode ser uma boa mãe.

Mesmo que uma rede utilize um sistema operacional que contenha muitas falhas, os bons administradores todo dia estarão checando por falhas descobertas e corrigindo-as. Já os outros provavelmente vão ficar em algum chat comendo sanduíches.

Sistemas operacionais

Como eu disse anteriormente, não há realmente um sistema que seja melhor que o outro. Existem vantagens e desvantagens de cada um. Tudo bem que alguns possuem erros muitos grandes, mas podem facilmente ser corrigidos. A intenção do sistema também importa. Não adianta ter uma rede e utilizar Windows 98 ou ME. Os recursos de segurança deles são muito escassos, pois foram feitos para o usuário comum e não para o ambiente empresarial. Não adianta também instalar o **Digital Unix**, **FreeBSD** ou **AIX** se o seu administrador só possui experiência em **Lantastic**. O sistema também vai depender do tipo de rede que você terá. Se você terá um servidor Web ou algum tipo de acesso externo, seria melhor utilizar o **Linux** ou o **Windows NT**. Se for uma rede interna somente, utilize **Novell Netware**, que ainda não fez a sua história quanto à Internet, mas ainda é insuperável nas redes locais.

A segurança ao longo da história

Anos atrás, os operadores de um computador ENIAC se depararam com uma coisa curiosa. Um inseto havia ficado preso dentro da máquina e estava atrapalhando o funcionamento da mesma. Daí surgiu o termo **bug** (inseto) que virou sinônimo de falha. Hoje quando se descobre um erro em algum programa, se diz: "*novo bug descoberto*". De lá pra cá, as coisas evoluíram muito, mas os bugs continuam a existir. Muitos deles são frutos da história do próprio programa ou sistema. O Windows por exemplo. O Windows NT foi construído a partir do zero, mas o Windows ME não. Desde o início da criação de sua primeira interface gráfica, a Microsoft vêm tendo problemas com erros graves em seu sistema operacional. Já o sistema Unix, foi criado pelos desenvolvedores da linguagem C, para ser um sistema versátil e poderoso. Para conhecer melhor sobre a história de cada sistema, leia a seção sistemas operacionais .

A Internet também têm seus problemas ligadas à história de sua origem. Desde que se chamava Arpanet e foi criada pelo exército americano para resistir à guerra fria, a rede evoluiu muito e foram criados novos serviços como **E-mail**, **World Wide Web**, **Gopher**, **Wais** e outros. Milhões de computadores se juntaram a ela e seus recursos são cada vez mais sofisticados. Mas alguns problemas bem antigos ainda prejudicam hoje. Uma falha na implementação do TCP/IP(conjunto de protocolos em que a Internet se baseia) por exemplo, possibilita que o ataque de **Spoof** aconteça.

Invasores digitais

Todos os dias surgem notícias sobre piratas digitais na televisão e na Internet. Um pirata invadiu o computador de um sistema de comércio eletrônico, roubou os números de cartão, comprou Viagra e mandou entregar na casa do Bill Gates. Outro conseguiu derrubar sites famosos como YAHOO, CNN, AMAZON e ZDNET. Mais recentemente um grupo estrangeiro conseguiu tirar mais de 650 sites do ar em um minuto. Para entender como se organiza a hierarquia virtual da Internet, vamos estudar seus principais integrantes:

Hackers

Na verdade, os hackers são os bons mocinhos. Para os fãs de Guerra nas Estrelas, pensem no hacker como o cavaleiro jedi bonzinho. Ele possui os mesmos poderes que o jedi do lado negro da força (cracker) mas os utiliza para proteção. É um curioso por natureza, uma pessoa que têm em aprender e se desenvolver um hobby, assim como ajudar os "menos prevalecidos". Um bom exemplo real foi quando o cracker *Kevin Mitnick* invadiu o computador do analista de sistemas *Shimomura*. Mitnick destruiu dados e roubou informações vitais. Shimomura é chamado de hacker pois usa sua inteligência para o bem, e possui muitos mais conhecimentos que seu inimigo digital. Assim facilmente montou um **honeypot** (armadilha que consiste em criar uma falsa rede para pegar o invasor) e pegou Kevin. Infelizmente a imprensa confundiu os termos e toda notícia referente a baderneiros digitais se refere à hacker.

Essa é a imagem do hacker que você deve ter.

Crackers

Esses sim são os maldosos. Com um alto grau de conhecimento e nenhum respeito, invadem sistemas e podem apenas deixar a sua "marca" ou destruí-los completamente. Geralmente são hackers que querem se vingar de algum operador, adolescentes que querem ser aceitos por grupos de crackers (ou script kiddies) e saem apagando tudo que vêem ou mestres da programação que são pagos por empresas para fazerem espionagem industrial. Hackers e crackers costumam entrar muito em conflito. Guerras entre grupos é comum, e isso

pode ser visto em muitos fóruns de discussão e em grandes empresas, as quais contratam hackers para proteger seus sistemas.

O Darth Maul representa bem um cracker

Os hackers e crackers são eternos inimigos. Um não gosta do outro e sempre estão lutando por seus ideais. Usei a analogia do guerra nas estrelas pois expressam exatamente bem pessoas de poderes iguais mas de ideologias opostas. Nossos invasores digitais são assim: mocinhos e vilões brigando. E brigas feias.

Phreakers

Maníacos por telefonia. Essa é a maneira ideal de descrever os phreakers. Utilizam programas e equipamentos que fazem com que possam utilizar telefones gratuitamente. O primeiro phreaker foi o *Capitão Crunch*, que descobriu que um pequeno apito encontrado em pacotes de salgadinhos possui a mesma freqüência dos orelhões da AT&T, fazendo com que discassem de graça. Um programa comum utilizado é o blue box, que gera tons de 2600 pela placa de som, fazendo com que a companhia telefônica não reconheça a chamada. Também têm o Black Box que faz com que você possa ligar de graça do seu telefone doméstico e o

Red Box que possibilita que se ligue de orelhões. Se quiser saber mais sobre o assunto, consulte o site www.txt.org .

Outra técnica muito usada principalmente no Brasil é a de utilizar um diodo e um resistor em telefones públicos. Ou de cobrir o cartão telefônico de papel alumínio para que os creditos não acabem (nunca testei, mas me disseram que funciona). Técnicas como essas são utilizadas no mundo inteiro. O phreaker é uma categoria à parte, podem ser hackers, crackers ou nenhum dos dois. Alguns phreakers brasileiros são tão avançados que têm acesso direto à centrais de telefonia, podendo desligar ou ligar telefones, assim como apagar contas. Um dos programas muitos usados para isso é o **ozterm**, programinha de terminal que funciona em modo dos. Por sinal, muito difícil de encontrar na net.

Funcionários

Outro problema grave. 60% das invasões hoje acontecem de dentro da própria empresa, por funcionários insatisfeitos ou ex-funcionários que querem vingança. Utilizam-se do conhecimento adquirido e arrasam com dados do sistema. Copiam coisas do seu interesse (como o banco de dados que possui o telefone da loira do setor B) ou instalam joguinhos em rede que podem comprometer a segurança, pois com certeza não se preocupam em passar anti-vírus. Utilizam trojans, scanners e sniffers para capturar o que lhes interessa. Firewall é ineficaz contra eles. Afinal, do que adianta a grande muralha da china se algum soldado é o traidor?

Mitos e fantasias

O maior mito existente na Internet é que o cracker pode invadir qualquer computador na hora que quiser. Não é bem assim. Invasões por ICQ por exemplo, pura besteira. Só era possível em versões antigas e mesmo assim se o servidor web que vêm com o programa estivesse ativo. Isso porquê para conseguir acesso ao interpretador de comandos do sistema por alguma porta, têm de existir um serviço próprio para isso. Para se invadir um computador pessoal, só existem duas maneiras: trojans e netbios. A não ser que seja um computador que rode muitos serviços (FTP, Web, Telnet), o perigo é mínimo.

Outro mito é o que o hacker e o cracker são vistos como gênios da informática. Bom, os de antigamente realmente eram e ainda existem alguns poucos mas a grande maioria que se diz “hacker” hoje em dia se aproveita das ferramentas encontradas na Internet. Nem programar sabem. São os famosos **Script Kiddies**, sub-categoria de crackers. Não têm um alvo certo, vão tentando invadir tudo que vêm na frente. Pior que eles só os **Lamers**, aqueles que chegam nos chats anunciando “vou te invadir, sou o melhor” mas acaba desistindo pois não consegue descompactar nem um arquivo ZIP.

Engenharia social

A engenharia social é uma tática muito usada pelos crackers, desde o início dos tempos. É o que a lei chama de estelionato. Consiste em enganar uma pessoa para se conseguir vantagens. Como no caso do indivíduo que liga para o provedor e pergunta: “Por favor, perdi minha senha de Internet. Poderia olhá-la para mim?”. Alguns provedores pedem documentação para comprovar que é o dono da conta, outros (com funcionários insatisfeitos em sua maioria) não ligam, passam até o número do cartão de crédito de algum usuário se lhe pedirem. Esse método é utilizado também para conseguir informações sobre uma certa pessoa.

Vá a uma companhia telefônica e peça a segunda via de um telefone qualquer. Na grande maioria das vezes não lhe pedem documento e você consegue o endereço residencial de qualquer pessoa. Alguns filmes como *Hackers* e *Caçada Virtual* mostram bastante essa técnica.

Como conseguir uma política eficiente de proteção

Leia muito sobre as novidades do mundo da segurança. Veja se o seu administrador realmente se preocupa com a proteção do sistema ou contrate alguém somente com essa função. Faça sempre backup dos logs e varredura do sistema por falhas. Cheque o computador dos funcionários procurando por programas escondidos e passe um bom anti-vírus neles. Se for usar algum programa de segurança, como firewalls, detectores de invasão e outros, dê preferência para aqueles mais conhecidos e confiáveis.

Tenha certeza de que quando despedir alguém, mudar as senhas de acesso ao sistema. Nunca discuta com um cracker (para o seu próprio bem). E o mais importante: saiba que apesar de tudo isso, nunca vai estar totalmente seguro. Nenhum sistema é 100% à prova de falhas. Mas pelo menos você pode diminuir muito o risco.

2

Analisando o nível de perigo

A influência do sistema operacional

Como vimos no capítulo anterior, o sistema operacional não influi tanto na segurança quanto algumas pessoas pensavam. Citei anteriormente que se alguém precisasse de um servidor externo seria melhor que utilizasse o Linux ou o Windows NT se fosse apenas uma rede local. E o Netware? A Novell passou a apostar na Internet recentemente, suas antigas versões não possuem o suporte devido à rede. E os seus servidores web ainda não são tão utilizados em larga escala quanto o Apache e o IIS. Por isso não nos aprofundaremos muito nele, pois nosso principal foco são os ataques remotos. Leia um pouco mais sobre cada um.

Unix versus Windows

Por serem os dois sistemas mais usados quando se utiliza servidores externos(servidores de e-mail, , abordaremos uma breve explicação sobre suas diferenças. Para mais detalhes ver a seção **sistemas operacionais**. O Unix é multi-tarefa e o Windows também. Ambos são largamente usados hoje em dia, sendo distribuídos em várias variantes (Linux, Xenix, Windows ME, Windows XP). O Windows possui algumas vantagens sobre o Unix. Mais simples de se usar, é fácil de se instalar programas e drivers, e possui mais programas no mercado. Apenas isso. O Unix em comparação, possui inúmeras vantagens sobre o Windows. Vamos listar algumas.

- Têm distribuções gratuitas (como é o caso do Linux)
- Criptografia inquebrável de senhas. Só se descobre no método da tentativa e erro.
- Melhores ferramentas de rede
- Melhor gerenciamento de permissões
- Código-fonte aberto

Vantagens do *open source*

As vantagens do código-fonte aberto (ou open-source) são muito grandes. Esse termo significa que os programas criados (ou o próximo sistema operacional) vêm junto com o seu código fonte, ou seja, você pode ver exatamente o que está executando. Para começar, qualquer um pode fazer sua própria versão de Unix ou Linux. É só pegar o código fonte de algum sistema já existente e alterá-lo. Como o sistema operacional foi feito de programadores

para programadores, ainda possuem alguns recursos que o usuário comum não consegue entender. Mas até isso o open-source está mudando. Novas ferramentas gráficas foram criadas para facilitar o uso do Unix. Podem torná-lo tão fácil de usar quanto o Windows. E o melhor são melhoradas rapidamente pelos seus próprios usuários e distribuidas gratuitamente. Alguns bons exemplos são o GNOME e o KDE, os ambientes gráficos mais usados na atualidade.

Configurações malfeitas

A configuração malfeita é a perdição de um bom sistema. Contas padrões, serviços desnecessários ativos e erros em permissões de arquivos são falhas muito grandes. As contas padrões são perigosas pois todo mundo conhece sobre elas. O caso do Unix por exemplo. Contas como **bin** e **admin** vêm com senhas padrões de acesso ao sistema. Desabilite-as ou mude as senhas. Quanto aos serviços, se você possui um servidor telnet, ou mesmo ftp, que estiver usando pouco, desabilite-os. Ou pelo menos configure para esse servidor as relações de confiança dizendo qual endereço IP poderá ter acesso a ele e qual o acesso será restrito. As permissões de arquivo também são importantes. Elas impedem que alguém execute algum programa malicioso ou acesse o arquivo de senhas.

Ataques restritos a um tipo de sistema

Todo sistema sofre ataques de maneiras diferentes. E alguns desses ataques afetam o sistema ou não causam absolutamente nada. Um bom exemplo é o caso dos vírus e trojans. Para Unix, eles praticamente não existem. Mas para Windows há milhões deles. O Unix possui falhas em alguns servidores que o Windows não, como o sendmail. O melhor arma para invadir algum sistema é ele mesmo. Por exemplo, se quero conseguir acesso a um servidor Linux, dificilmente conseguirei utilizando Windows NT.

Ataques universais intra-sistemas

São ataques em que não importa o tipo do SO (Sistema Operacional) de origem ou de destino. Funciona em todos os sistemas. Como é o caso do IP Spoof. Ele trabalha a nível de protocolo, utilizando-o você consegue acesso a qualquer máquina, seja Windows, Unix, Novell, DEC-10, VMS, o que for.

Recusa de serviço e invasão

Existem apenas dois tipos de ataques que um sistema pode sofrer. O primeiro é o Denial of Service (DoS) ou Recusa de serviço. Esse ataque consiste em inundar a máquina alvo com dezenas de pacotes de informação, fazendo com que ela não consiga processar a todos e consuma toda a sua memória, paralizando-a. Esse ataque apenas causa danos temporários, como tirar o servidor do ar, mas não fornece acesso aos arquivos. É como se um ladrão, vendo que não vai conseguir roubar um carro, fure os quatro pneus. É chato, demora pra arrumar os pneus mas pelo menos o cd player e os documentos do carro não foram levados. Já a invasão é diferente. Consiste em procurar e utilizar alguma falha do sistema contra ele próprio. Ou então instalar programas residentes na memória (trojans ou sniffers) para que monitorem todo o tráfego de senhas e forneçam acesso a arquivos importantes.

Protocolos , ferramentas de rede e footprinting

3

Protocolos

Esse capítulo foi feito para quem quer entender um pouco mais sobre protocolos de rede e como eles funcionam. Se você não têm nenhum interesse em dados teóricos, pule o capítulo. Protocolos são programas e devem ser instalados em componentes de rede que precisam deles. Computadores só podem comunicar-se entre si se utilizarem o mesmo protocolo. Se o protocolo usado por um computador não for compatível pelo usado em outro, eles não podem trocar informações. Uma variedade de protocolos está disponível para uso em sistemas de rede fechados (como Novell Netware)

Tipos de protocolos

Dois tipos de protocolos existem hoje: abertos e específicos.

Protocolos Abertos

Protocolos abertos são protocolos feitos para o padrão da indústria. Eles se comunicam com outros protocolos que utilizam o mesmo padrão. Um protocolo aberto não possui dono e todos os sistemas podem fazer implementações livremente. Um ótimo exemplo do que é um protocolo aberto é o TCP/IP (Transfer Control Protocol / Internet Protocol). Ele é composto por muitos outros protocolos e está implementado em muitos sistemas (como Macintosh, Windows, Linux, Unix, etc...). O TCP/IP é o protocolo padrão da Internet.

Protocolos Específicos

Protocolos específicos são feitos para ambientes de redes fechados e possuem donos. Como é o caso do IPX / SPX que foi desenvolvido especificamente para a estrutura Novell Netware.

Tipos de transmissão de dados

Protocolos roteáveis permitem a transmissão de dados entre diversos segmentos de uma rede. O problema é que o grande volume de certo tipo de tráfego (como executar uma aplicação multimídia pesada) deixa a velocidade de conexão muito lenta. A quantidade de tráfego gerada em uma rede, pode ser de três tipos: Unicast, Broadcast e Multicast.

Unicast

Em uma transmissão unicast, uma cópia separada dos dados são enviados de sua origem para cada computador cliente que os requeste. Nenhum outro computador na rede precisa processar o tráfego gerado. No entanto, em uma rede com muitos computadores o unicast não é muito eficiente pois o computador de origem terá que transmitir múltiplas cópias dos dados (resultado, ficará lento). O unicast é bom de ser usado apenas em pequenas redes.

Broadcast

Esse é o tipo de transmissão preferido da turma que gosta de um Denial of Service. Nesse tipo de transmissão, os dados são enviados apenas uma vez mas para toda a rede. Esse processo não é muito eficiente pois faz a velocidade cair bastante já que todos os computadores irão receber os dados. Mesmo os hosts que não fizeram o pedido receberão os dados. Somente não irão processá-los. Esse método é utilizado no ataque de smurf, em que é enviado um broadcast para diversos endereços IP e o endereço de origem (que deveria ser o IP de quem enviou) é modificado para o da vítima. Resultado: centenas de máquinas mandarão milhares de unicasts para um pobre coitado.

Multicast

É uma mistura dos dois. É enviada apenas uma cópia dos dados e somente os computadores que fizeram o pedido os recebem, assim evitando de se causar um tráfego muito intenso e consequentemente um congestionamento na rede. Muitos serviços de Internet usam multicast para se comunicar com computadores clientes (quando se diz cliente , é o computador que faz o pedido, que espera uma resposta). Inclusive é nesse tipo de comunicação que se baseia o protocolo IGMP.

NetBios

A interface NetBIOS (NetBEUI) foi um dos primeiros protocolos disponíveis para uso em redes compostas de computadores pessoais. Como o próprio nome diz, o **NET**work **B**asic **I**nput **O**utput **S**ystem, foi designado para ser um protocolo eficiente e pequeno para uso em redes caseiras não roteadas de cerca de no máximo 200 computadores.

Atualmente o NetBIOS é usado mais exclusivamente em pequenas redes não-roteadas podendo ou não estar rodando em vários sistemas operacionais. A implementação NetBIOS do Windows é chamada de NetBEUI. As suas vantagens incluem:

- Grande velocidade de transferência
- Nenhuma necessidade de configuração
- Compatibilidade com praticamente todos os sistemas operacionais, inclusive o Linux (usando o Samba).

A única desvantagem é que o NetBIOS não suporta roteamento. Trocando em miúdos: o máximo que você vai conseguir invadir usando esse protocolo é o computador do seu

primo ou de sua namorada que usam o mesmo provedor que você. Se for um provedor diferente, esqueça (a não ser que seja o NBT ao invés do SMB, como foi explicado anteriormente). Outro problema: a estrutura de segurança do NetBIOS é extremamente pobre. Facilmente podemos quebrar as senhas utilizados (usando bruteforce). Além do Shadow Scan já citado anteriormente, o NAT (NetBIOS Auditing Tool) também é uma ótima ferramenta para fazê-lo.

Alguns bugs também são facilmente encontrados, como a má configuração do IPC$ do Windows NT. Aliás, pense um pouco nesta pergunta: por quê o NetBIOS do Windows NT possui o compartilhamento IPC$ padrão, o Windows 9x possui o $printer (que possibilita cair no Windows\System usando o compartilhamento de uma impressora) e o Linux não possui nenhum desses? Qual o objetivo desses compartilhamentos? Fiz essa pergunta a um formando de Ciências da Computação e ele não soube me responder. Existem duas respostas, uma longa e uma curta. A longa deixarei para a análise pessoal de cada um. Já a curta é simples: o Linux é bem mais seguro.

Para se resolver nomes NetBIOS, podem ser usadas três maneiras:

1. **Arquivo LMHOSTS**
2. **Broadcast**
3. **WINS**

Vamos analisar o método do LMHOSTS que creio ser o mais simples de todos. Ele consiste na tradução de endereços NetBIOS em endereços IP, somente configurando o arquivo lmhosts. O arquivo não possui extensão e pode ser encontrado nos diretórios dos seguintes sistemas:

UNIX *./etc*

Mac OS X *System Folder*

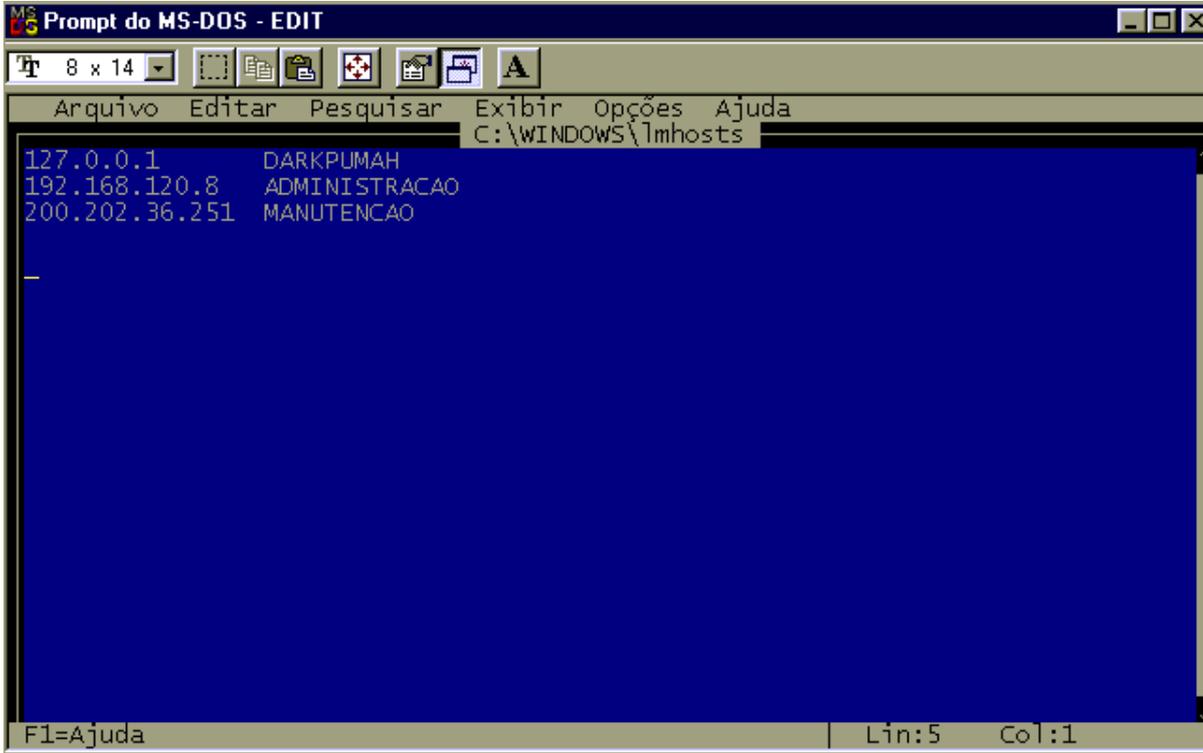
Windows 9X *c:\windows (ou onde o Windows foi instalado)*

Windows NT *c:\winnt\System32\Drivers\Etc*

O arquivo deve ser criado utilizando a seguinte sintaxe:

< endereço IP> espaço <nome NetBIOS>

Esse é o modo mais simples de criação do arquivo. Podem-se adicionar comentários utilizando o caractere #. Atenção: não confundir arquivo LMHOSTS com HOSTS (visto em TCP/IP).

Um exemplo de arquivo LMHOSTS:

Nesse exemplo criamos um arquivo simples, ligando três endereços IP a nomes NetBIOS. Observe que o primeiro é o endereço de local (o chamado loopback). Leia mais sobre endereço na seção sobre TCP/IP

Há dois tipos de ambiente NetBIOS: Único e grupo. Um nome único deve ser único através da rede (um usuário por exemplo). Um nome de grupo não precisa ser único e processa informações de todo um grupo de trabalho. Cada nó NetBIOS mantêm uma tabela de todos os nomes possuidos por ele. A convenção do nome NetBIOS possibilita que se crie nomes com 16 caracteres. A Microsoft, entretando, limita esses nomes para 15 caracteres e usa o 16º caracter como um sufixo NetBIOS. Um sufixo NetBIOS é usado pelo software de rede da Microsoft para identificar o serviço que está rodando.

Nota: SMB e NBT (NetBIOS sobre o TCP/IP, alguns o chamam apenas de SMB por TCP/IP) funcionam de modo muito parecido e ambos usam as portas 137, 138, 139. A porta 137 é o nome NetBIOS por UDP. A port 138 é o datagrama NetBIOS por UDP. E a port 139 é a sessão NetBIOS por TCP. Mas o NBT costuma usar a porta 445 também.

The following is a table of NetBIOS suffixes currently used by Microsoft WindowsNT. These suffixes are displayed in hexadecimal format.

Nome **Número** **Tipo** **Uso**
==

<nome_do_computador>	**00**	**U**	**Serviço de workstation**
<nome_do_computador>	**01**	**U**	**Serviço de mensagens**
<_MSBROWSE_>	**01**	**G**	**Browser principal**
<nome_do_computador>	**03**	**U**	**Serviço de mensagens**
<nome_do_computador>	**06**	**U**	**Serviço de servidor RAS**
<nome_do_computador>	**1F**	**U**	**Serviço NetDDE**
<nome_do_computador>	**20**	**U**	**Serviço de servidor de arquivos**
<nome_do_computador>	**21**	**U**	**Serviço de cliente RAS**
<nome_do_computador>	**22**	**U**	**Trocas de intercomunicação**
<nome_do_computador>	**23**	**U**	**Trocas de Armazenamentos**
<nome_do_computador>	**24**	**U**	**Diretórios do Exchange**
<nome_do_computador>	**30**	**U**	**Servidor de compart. de modem**
<nome_do_computador>	**31**	**U**	**Cliente de compart. de modem**
<nome_do_computador>	**43**	**U**	**Cliente remoto SMS**
<nome_do_computador>	**44**	**U**	**Admin remoto SMS**
<nome_do_computador>	**45**	**U**	**Chat remoto SMS**
<nome_do_computador>	**46**	**U**	**Transferência remota SMS**
<nome_do_computador>	**4C**	**U**	**Serviço TCP/IP DEC**
<nome_do_computador>	**52**	**U**	**Serviço TCP/IP DEC**
<nome_do_computador>	**87**	**U**	**Exchange MTA**
<nome_do_computador>	**6A**	**U**	**Exchange IMC**
<nome_do_computador>	**BE**	**U**	**Agente monitor da rede**
<nome_do_computador>	**BF**	**U**	**Software monitor da rede**
<usuário>	**03**	**U**	**Serviço de mdensagens**
<domínio>	**00**	**G**	**Nome de domínio**
<domain>	**1B**	**U**	**Browser de domínio**
<domain>	**1C**	**G**	**Controlador de domínio**
<domain>	**1D**	**U**	**Browser principal**
<domain>	**1E**	**G**	**Serviços do browser**
<INet~Services>	**1C**	**G**	**Internet Information Server**
<IS~Computer_name>	**00**	**U**	**Internet Information Server**
<nome_do_computador>	**[2B]**	**U**	**Servidor Lotus Notes**
IRISMULTICAST	**[2F]**	**G**	**Lotus Notes**
IRISNAMESERVER	**[33]**	**G**	**Lotus Notes**
Forte_$ND800ZA	**[20]**	**U**	**Serviço de gateway DCA**

As denominações mais importantes para nós aqui são:

Único (U): O nome pode ter apenas um endereço IP ligado a ele. Em uma rede, múltiplas ocorrências de nomes simples podem parecer estarem registradas mas o sufixo será único (em outras palavras, pode parecer um grupo mas não é)

Group (G): Um grupo normal; o nome simples pode existir com muitos endereços IP.

IPX/SPX

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) é um protocolo desenvolvido especificamente para a estrutura Novell NetWare. O IPX define o endereçamento da rede NetWare e o SPX fornece segurança e confiabilidade ao IPX. (O SPX

é como aqueles caras que só se sentem seguros ao lado da esposa). Para comparação, o IPX é como se fosse o IP do protocolo TCP/IP (visto mais à frente).

O IPX/SPX possui as seguintes características:

- São usados com servidores NetWare
- São roteavéis, permitem que os computadores em um ambiente de rede trocam informações através de segmentos.

AppleTalk

Protocolo criado pela apple para utilização em redes macintosh para o compartilhamento de arquivos e impressoras. É componente específico, ou seja não é um padrão do mercado. As duas principais características do AppleTalk são:

1. Possibilita clientes Macintosh acessarem servidores Windows NT
2. É roteável. (pode se comunicar com redes externas, tal como o IPX/SPX e o TCP/IP)

TCP/IP

Sem dúvida o melhor dos protocolos. Quando alguém chega a mim e diz que se converteu ao TCP/IP, creio que sinto o mesmo prazer de um crente que consegue levar o amigo à sua igreja. Diferente dos outros protocolos vistos aqui, o TCP/IP na verdade é um conjunto de muitos protocolos. Usando uma arquitetura cliente-servidor quase perfeita, esse conjunto de protocolos possibilita praticamente todo tipo de sistema operacional e rede de se comunicarem entre si, possibilitando até a criação da Internet. Ora, como seria possível um monte de computadores usando Macintosh, Unix , Linux e Windows comunicarem-se sem maiores problemas? Não, não é um filme de Hollywood e muito menos um sonho distante. É a tecnologia a nosso serviço. E o melhor de tudo, é um protocolo aberto.

Para começarmos o nosso estudo sobre os protocolos que compõem o TCP/IP, analisemos um a um os mais importantes deles. Ou em outras palavras, os que mais iremos utilizar. Não dá para vermos todos pois além de serem muitos, têm de ser estudados a fundo. Apenas darei uma noção.

IP

O IP (Internet Protocol) é o responsável por rotear e entregar os pacotes contendo as informações que serão enviadas. O endereço IP contém um cabeçalho aonde estão indicados os endereços de redes e de hosts. Esse endereço é representado por quatro bytes separados por pontos. Por exemplo:

200.202.36.251

As duas primeiras partes (200.202) indicam o endereço da rede. Ou seja, provavelmente todos os hosts dessa rede começam com esse endereço. O que vai mudar de host para host é a parte final do endereço (36.251). Claro que isso não é uma regra, existem redes gigantescas em que essas propriedades podem mudar. Para saber se qual o endereço de rede e o endereço de host de uma rede, cheque a **máscara de sub-rede**.

A máscara de sub-rede (subnet mask) nos informa quais àreas do ip são mutáveis (usadas por hosts) e quais não mudam. Exemplo:

255.255.255.0

O que isso significa? Quando uma área da máscara de sub-rede tiver o número 255, significa que aquela àrea é imutável e quando for 0 a àrea pode mudar. Achou difícil? Não é. Preste atenção: observando o endereço acima, dá para notarmos o quê? Que somente a última parte do endereço IP está com o zero. Supondo que o endereço IP de uma máquina da rede seja **200.131.16.1** .Provavelmente existirão hosts com esses endereços:

200.131.16.2

200.131.16.3

200.131.16.4

200.131.16.5

Mas não existirão máquinas com esses endereços:

200.131.63.1

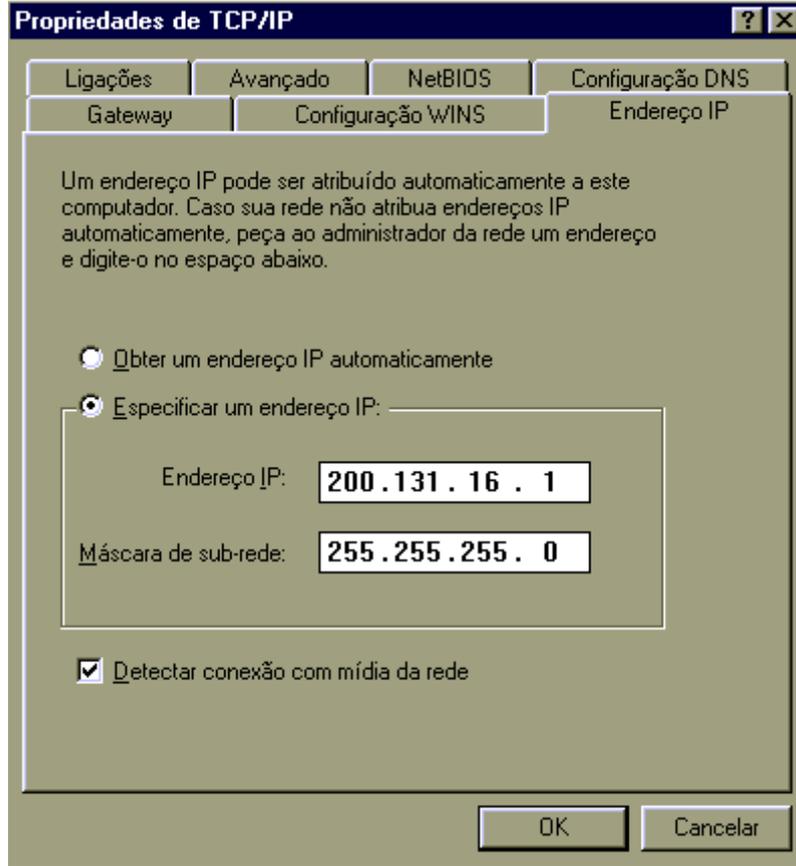
200.131.65.6

200.131.19.4

200.131.33.66

Por quê? Porquê como a máscara de sub-rede foi configurada para **255.255.255.0**, somente o último byte do ip pode ser alterado. Agora, se a máscara for mudada para **255.255.0.0**, os endereços ip acima seriam aceitos pois os últimos dois bytes (as duas últimas àreas separadas por pontos) podem ser mudados. Nas propriedades de TCP/IP (que variam de um sistema operacional para o outro) você encontra a máscara de sub-rede.

No Windows, siga os seguintes passos:

1. Clique em **Iniciar** e vá em **Configurações** e **Painel de Controle**
2. Procure entre os ícones o de **Rede e** clique duas vezes para acessá-lo
3. Na lista de protocolos, procure o **TCP/IP** e clique em propriedades
4. Em propriedades de TCP/IP, clique em **Endereço IP**

5. Agora selecione **especificar um endereço IP** e coloque como teste o endereço **200.131.16.1**
6. Escreva a máscara de sub-rede desejada abaixo.
7. Não se esqueça depois de que se anteriormente a opção de **obter um endereço IP automaticamente** estava habilitada, habilite-a antes de sair.

Propriedades do protocolo TCP/IP

No endereço IP os números podem variar de **0 a 255** , mas geralmente em hosts são utilizados apenas de **1 a 254**. O **0** e o **255** são usados apenas para a máscara de sub-rede.

Portas

Se você quisesse colocar um servidor de homepage e um servidor de jogos em um host tendo um só endereço IP seria impossível. Como o cliente saberia identificar qual dos servidores precisa se conectar? Para isso criaram as **portas**. Elas identificam conexões utilizando números de 0 a 65536. Alguns serviços já possuem até suas portas padrões, como é o caso do Telnet (porta 23) e do FTP (porta 21). Para saber quais serviços existem em um servidor, leia a seção sobre scanners para saber como scannear portas.

DNS

Nosso próximo passo no estudo do TCP/IP é o Domain Name Server (DNS) ou Servidor de Nome de Domínio, em português. A função dessa belezinha é extremamente útil. Já imaginou se você tivesse que decorar o endereço IP de todas as página que visita na Internet? No máximo uns 10 você decoraria, mas e o resto? Para acabar com esse problema surgiu o DNS. A sua função é procurar em um banco de dados um nome que corresponda a um IP. Quando digitamos **www.yahoo.com** por exemplo, não precisamos saber o endereço IP. O

DNS do nosso provedor de acesso vai checar esse nome em seu banco de dados e se encarregar de nos direcionar ao IP encontrado. Olha que protocolo bonzinho :-) .

Nós mesmo podemos configurar e ligar alguns nomes a endereços IP. O método mais fácil de se fazê-lo é utilizar o arquivo HOSTS. O processo é o mesmo do LMHOSTS do NetBIOS, e o arquivo é encontrado no mesmo local. O interessante do HOSTS é que você pode pregar peças nos seus amigos, direcionando endereços como **www.fbi.gov** para o IP de alguma homepage hackeada ou até seu endereço IP local e contar vantagem de que invadiu o FBI. Muitos "hackers" hoje em dia usam isso para aparecerem na televisão e "hackear" ao vivo.

SMTP

O Simple Mail Transfer Protocol é o protocolo responsável por entregar mensagens de e-mail a um destinatário. Toda vez que seus e-mails são enviados, um servidor smtp se encarrega de levá-los ao seu destino. Esse servidor geralmente se aloja na porta 25. O interessante do SMTP é que ao contrário do POP3 (visto a seguir), não é necessário senha para enviar um e-mail. Eu posso abrir o Microsoft Outlook e mandar e-mails como se fosse George Bush ou Tom Cruise. A falta de segurança no envio de mensagens é o ponto de partida para a facilidade de se enviar e-mails anônimos (como visto em anonimidade). O SMTP ainda permite anexar à uma mensagem de texto conteúdos binários (programas por exemplo), utilizando o MIME.

POP3

Outro protocolo de mensagens, só que agora é o responsável por o recebimento dessas mensagens. O POP3 já necessita de senhas para poder habilitar o acesso dos usuários às suas caixas postais, além de saber "re-montar" os arquivos enviados em formato MIME com o SMTP. O POP3 geralmente se localiza na porta 113. Uma grande desvantagem dele é que fica muito fácil fazer um ataque de bruteforce para tentar descobrir as senhas, já que a maioria dos servidores possui falhas que possibilitam softwares maliciosos de serem rodados.

TELNET

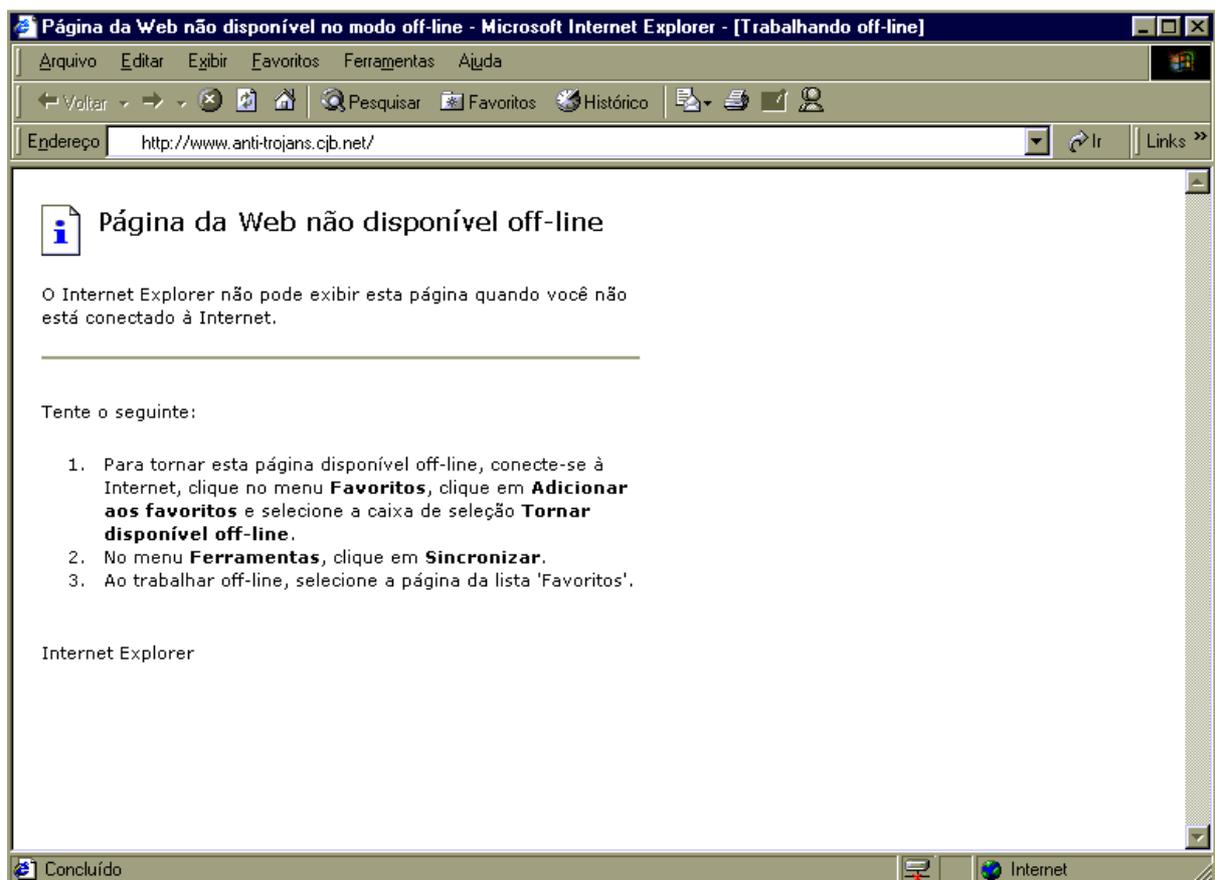
Telnet, ou terminal remoto é um modo de se acessar remotamente sistemas como se você os estivesse operando localmente. Por exemplo: usando o telnet (e um trojan instalado) podemos ter acesso ao MS-DOS de qualquer um. Do mesmo modo que poderíamos digitar comandos para listar, copiar e apagar dados, conectados a outro computador também podemos. Na verdade, todos os trojans são clientes telnet. Apenas são disfarçados com botõezinhos bonitinhos pois geralmente quem precisa de trojans para invadir sistemas são pessoas que não possuem um bom conhecimento de segurança. Se você encontrar alguma porta ativa em algum sistema (qualquer uma, seja de trojan, SMTP, POP3, etc...), pode se conectar a ela por telnet.

Resumindo, se você souber usar bem telnet não precisa mais de outros programas no computador. Ele acessa servidores utilizados pelos browsers (como Netscape e Internet Explorer), clientes de E-mail, IRC, absolutamente tudo. Leia sobre o cliente telnet do Windows no capítulo seguinte.

FTP

File Transfer Protocol é seu nome real. O protocolo de transferência de arquivos serve única e exclusivamente para ser um banco de software. Não se pode executar programas remotamente como no caso do telnet, apenas pegar e colocar arquivos. Desde a criação da Internet, o ftp é largamente usado. Uma de suas vantagens é, como ele é usado somente para transferências de arquivos, sua velocidade pode chegar a ser muito maior do que pegar arquivos em HTTP (visto mais à frente). No próximo capítulo você aprenderá os comandos básicos de um cliente FTP e como manipular os arquivos dentro deste.

HTTP

Esse sem dúvida é conhecido por muitos. Afinal, quem nunca viu na frente do endereço de uma homepage esse nome? **http://www.altavista.com/.** O Hyper Text Transfer Protocol é o protocolo responsável de transmitir textos, imagens e multimídia na Internet. Sempre que você abre uma homepage (mesmo que ele só contenha textos), você está usando esse protocolo. Achei interessante comentar sobre ele para que se entenda melhor como a Internet não funciona isolada com um só protocolo. HTTP, FTP, TELNET e os outros muitas vezes trabalham em conjunto e nem percebemos. Quando você for baixar um arquivo, preste atenção no link. É muito provável que de uma página navegada por HTTP, se envie a um servidor FTP.

Exemplo do protocolo http

SNMP

Simple Network Management Protocol. Algo como protocolo simples para manejar a rede. E é exatamente isso o que ele faz. Usando o SNMP você pode obter informações detalhadas sobre contas de usuário, equipamentos de rede, portas e serviços abertos e muito mais. A má configuração desse protocolo (deixando seu status como público principalmente). Use a ótima ferramenta IP Network Browser da SolarWinds (www.solarwinds.net). Ela mostra até a cor da cueca do administrador. Uma dica: se dá valor ao seu emprego desabilite o snmp.

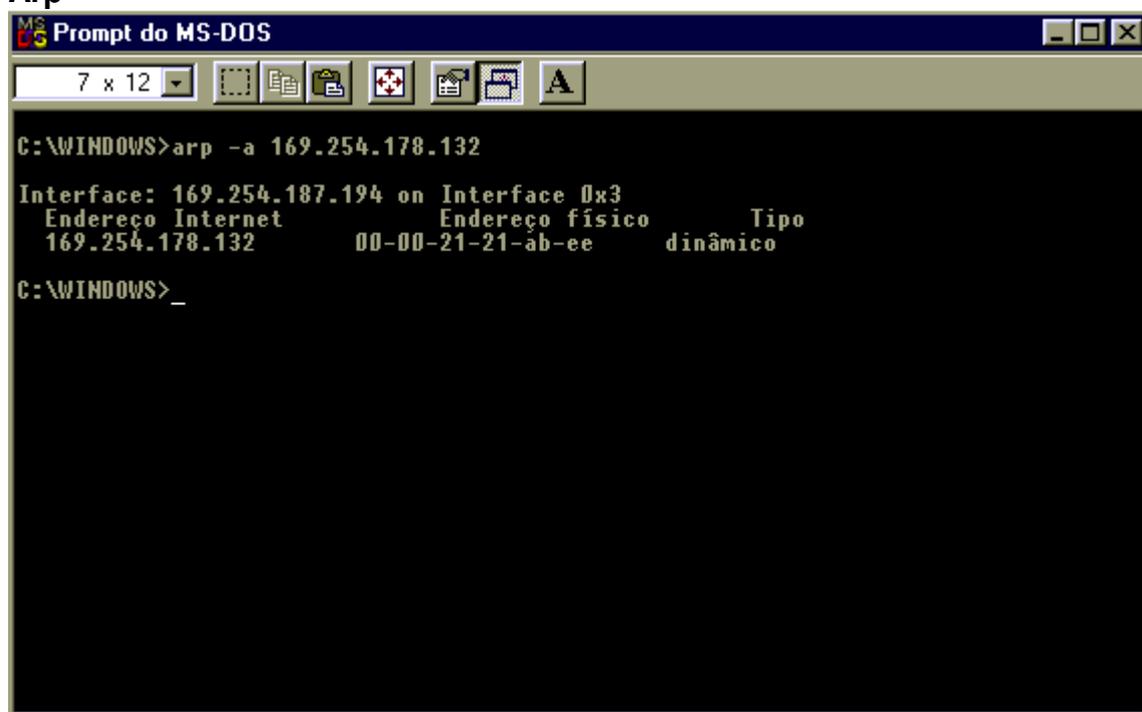
Screenshot do IP Network Browser

4

Ferramentas TCP/IP

Programinhas úteis

Existem muitos programas que vêm junto ao Windows e que possuem grande utilidade. A grande maioria deles também funciona em Linux e Unix (o que muda um pouco é apenas a sintaxe). Agora que já passei uma noção do que é o TCP/IP e como funcionam muitos de seus protocolos, ficará mais fácil de aprendermos sobre as ferramentas essenciais de rede. Será apresentada a ferramenta, uma tela de ilustração e sua sintaxe de uso. Como as ferramentas existentes são muitos, veremos apenas as mais importantes para nós.

Arp

```
Prompt do MS-DOS

C:\WINDOWS>arp -a 169.254.178.132

Interface: 169.254.187.194 on Interface 0x3
  Endereço Internet          Endereço físico        Tipo
  169.254.178.132       00-00-21-21-ab-ee      dinâmico

C:\WINDOWS>_
```

Permite realizar consultas e alterações na tabela de mapeamento entre endereços IP e endereços MAC do cache ARP.

arp -a [*endereçoIP*] [**-N** *IPInterface*]

arp -s *endereçoIP endereçoMAC* [*IPInterface*]

arp -d *endereçoIP* [*IPInterface*]

Parâmetro	**Descrição**
endereçoIP	Especifica o endereço IP a resolver ou alterar.
EndereçoMAC	Especifica o endereço MAC a acrescentar ao cache do ARP. O endereço MAC é composto por 6 bytes (expressos em notação hexadecimal) separados por hífen.
IPInterface	Especifica o endereço IP da placa de rede cuja tabela ARP deverá ser alterada. Por default, a primeira interface disponível será utilizada.

-a Exibe as entradas de cache do ARP. Se o *endereçoIP* tiver sido especificado, mostra somente a entrada referente a esse endereço.

-g O mesmo que **–a**.

-d Exclui do cache do ARP o host especificado por *endereçoIP*. Se *IPInterface* for especificado, exclui o host do cache da placa de rede indicada por *IPInterface*.

-s Acrescenta ao cache do ARP uma associação entre *endereçoMAC* e *endereçoIP*. Se *IPInterface* tiver sido especificado, acrescenta a associação no cache do ARP da placa. de rede indicada por *IPInterface.*

-N Especifica o endereço IP da placa de rede à qual o comando se aplica.

FTP

```
FTP
Auto
220-ela seja visitada por milhares de internautas.
220-
220-##########################
220-******* IMPORTANTE ******
220-##########################
220-
220-
220----
220- NÒo esqueþa que ap%s realizar suas operaþ§es, vocÛ deve limpar o cache de s
eu navegador (Shift + Atualizar)
220----
220-
220-
220-Atualize seu programa de FTP para apontar para:
220-
220-ftp.hpg.com.br
220---------------
220-
220-Nao utilize www.hpg.com.br, nem www.(seulogin).hpg.com.br.
220-
220-Obrigado,
220-Equipe hpG.
220-
220 Bem vindo ao servidor de ftp do hpG..
Usuário (cflow.hpg.com.br:(none)): anonymous_
```

Transfere arquivos de ou para um computador remoto.

ftp [**-v**] [**-d**] [**-i**] [**-n**] [**-g**] [**-s**:*nomearq*] [**-a**] [**-w**:*tamanho*] [*computador*]

O servidor ftp solicitará um usuário e a senha correspondente.
A maioria dos servidores FTP pode ser acessada por usuários não cadastrados, utilizando o usuário *Anonymous.*
Esse usuário não requer senha, mas muitos servidores solicitam como senha um endereço de e-mail.

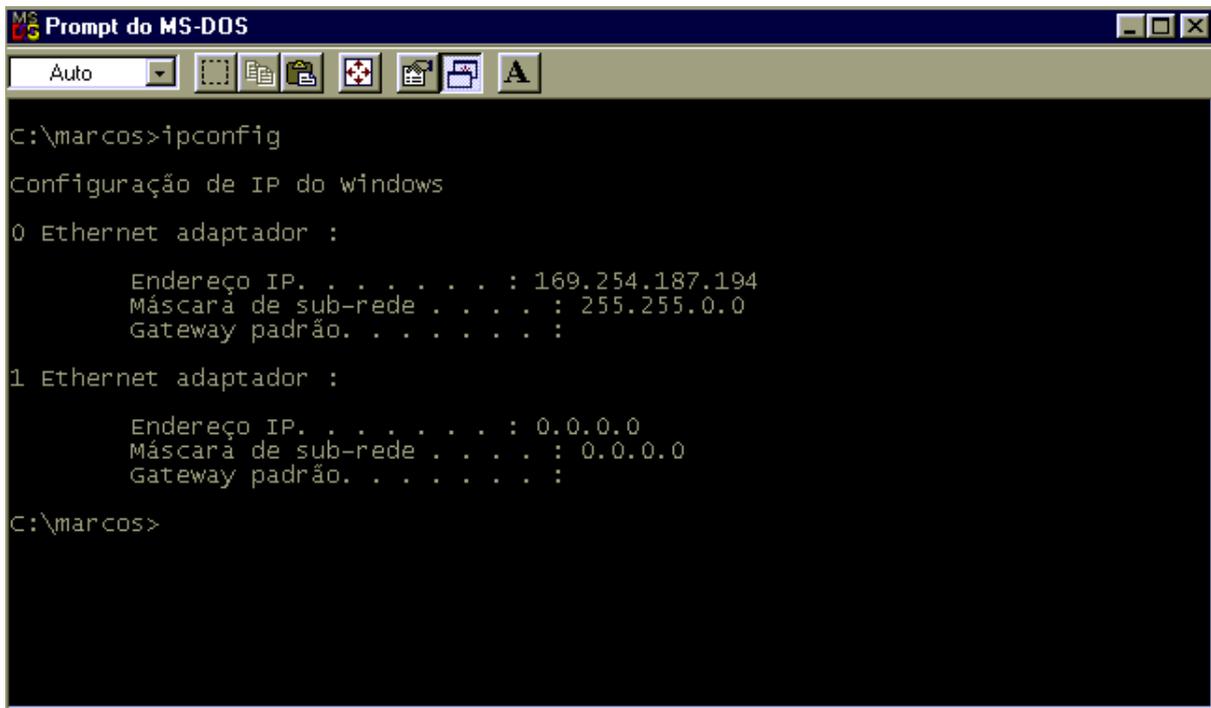
Opção	**Descrição**
-v	Elimina as mensagens de resposta do servidor.
-d	Ativa o modo de depuração, exibindo os comandos FTP enviados e recebidos.
-i	Desativa a confirmação para a transferência de cada arquivo em operações com múltiplos arquivos.
-n	Elimina o login automático na conexão inicial.
-g	Desativa o *globbing*, que permite o uso de caracteres de máscara (*, ?) em nomes de arquivos.
-s	Especifica um arquivo de texto contendo os comandos FTP a serem executados automaticamente.
-a	Utiliza qualquer placa de rede para estabelecer a conexão com o servidor FTP.
-w	Define o tamanho do buffer de transferência (o default é de 4 KBytes).
Computador	Nome do servidor FTP ou endereço IP. Deve ser o último parâmetro da linha de comando.

A seguir está a sintaxe dos comandos interativos do protocolo FTP. Esses comandos são utilizados de acordo com cada sistema e geralmente já com a conexão online.

Comando	**Descrição**
append	Acrescenta informações a um arquivo.
ascii	Indica que a transferência de arquivos será feita no modo de texto (arquivos apenas de texto, como TXT ou HTML)
bell	Emite aviso sonoro ao término do comando.
binary	Indica que a transferência de arquivos será feita no modo binário. (utilizado para arquivos não-texto, como fotos, programas e vídeos)

bye	Fecha a sessão FTP e sai do programa FTP.
cd	Seleciona um novo diretório de trabalho no computador remoto.
close	Fecha a sessão com um servidor FTP.
debug	Ativa/desativa o modo de depuração.
delete	Elimina arquivos no computador remoto.
dir	Lista o conteúdo de um diretório remoto.
disconnect	Fecha a sessão com um servidor FTP.
get	Copia um arquivo de um computador remoto para o computador local
glob	Ativa/desativa o uso de caracteres de máscara (*,?) em nomes de arquivos.
hash	Ativa/desativa a impressão de "#" para cada buffer transferido.
help	Exibe help on-line de um comando FTP. Se o comando não for especificado, exibe a lista dos comandos disponíveis.
lcd	Seleciona um novo diretório de trabalho no computador local.
literal	Envia uma linha de comando diretamente ao servidor FTP.
ls	Lista o conteúdo de um diretório remoto.
mdelete	Elimina múltiplos arquivos no computador remoto.
mdir	Lista o conteúdo de múltiplos diretórios no servidor remoto
mget	Copia múltiplos arquivos do computador remoto para o computador local.
mkdir	Cria um diretório no computador remoto.
mls	Lista o conteúdo de múltiplos diretórios no servidor remoto
mput	Copia múltiplos arquivos do computador local para o computador remoto.
open	Estebelece uma conexão com um servidor FTP.
prompt	Ativa/desativa a confirmação para a transferência com muitos arquivos
put	Copia um arquivo do computador local para um computador remoto (*upload*).
pwd	Exibe o diretório corrente no computador remoto.
quit	Fecha a sessão FTP e sai do programa FTP.
quote	Envia uma linha de comando diretamente ao servidor FTP.
recv	Copia um arquivo de um computador remoto para o computador local
remotehelp	Exibe help on-line para comandos diretos do servidor FTP.
rename	Renomeia um arquivo.
rmdir	Remove um diretório no computador remoto.
send	Copia um arquivo do computador local para um computador remoto (*upload*).
status	Exibe informações sobre a configuração do cliente FTP.
trace	Ativa/desativa o modo trace (exibição de todas as ações executadas).
type	Define ou exibe o tipo de transferência de arquivo (ASCII ou binary).

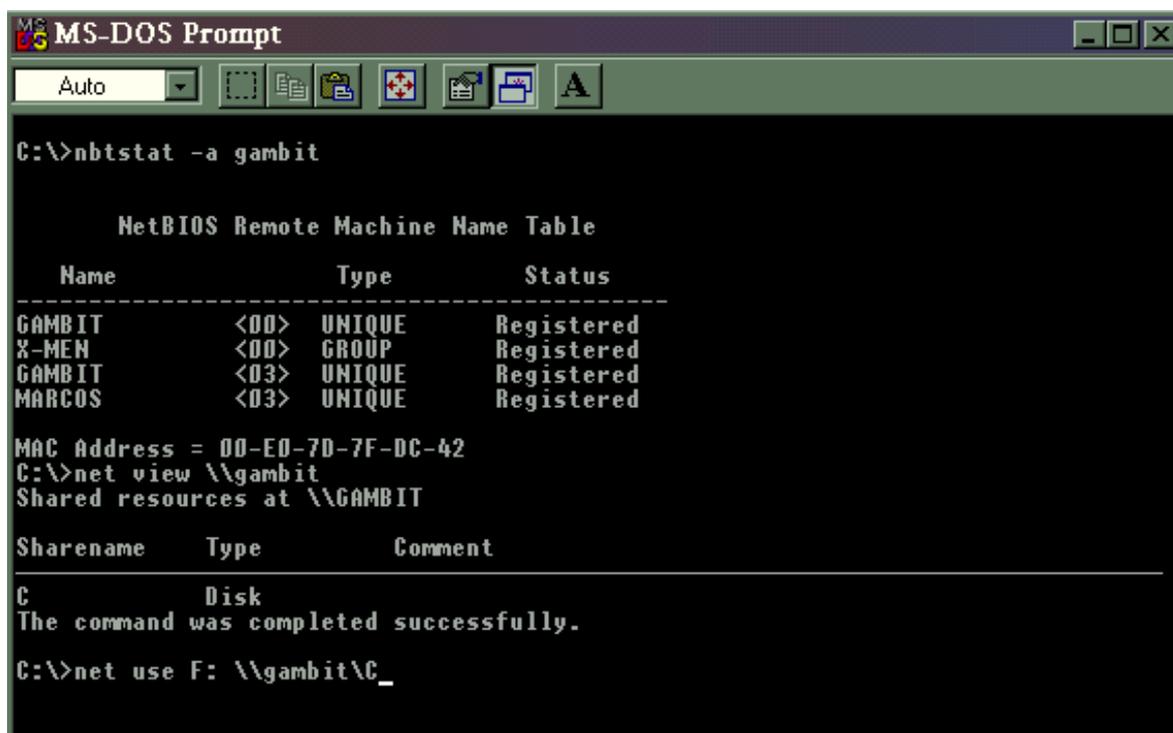
user Especifica um novo usuário para o computador remoto.

IPCONFIG

```
Prompt do MS-DOS

C:\marcos>ipconfig

Configuração de IP do Windows

0 Ethernet adaptador :

        Endereço IP. . . . . . . . : 169.254.187.194
        Máscara de sub-rede . . . . : 255.255.0.0
        Gateway padrão. . . . . . . :

1 Ethernet adaptador :

        Endereço IP. . . . . . . . : 0.0.0.0
        Máscara de sub-rede . . . . : 0.0.0.0
        Gateway padrão. . . . . . . :

C:\marcos>
```

Exibe a configuração do protocolo TCP/IP. Sem nenhum parâmetro, exibe os valores de endereço IP, máscara de sub-rede e *default gateway* para cada placa de rede instalada.

ipconfig [/? | /all | /release [*adaptador*] | /renew [*adaptador*]]

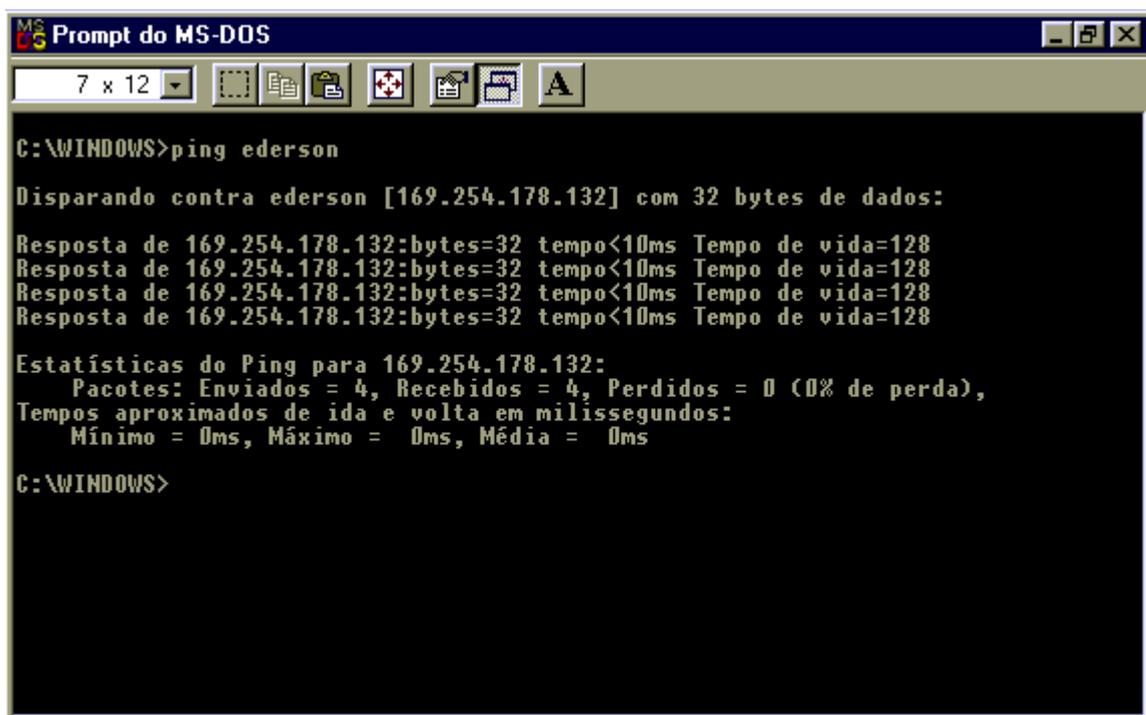
Opção	**Descrição**
/all	Exibe informações detalhadas de IP para as placas de rede instaladas. Além do endereço IP, da máscara de sub-rede e do *default gateway*,são exibidos também os endereços dos servidores DHCP, WINS e DNS para cada placa de rede instalada.
/release	Libera o endereço IP obtido para uma placa de rede através de um servidor DHCP. Se a placa de rede não for especificada, libera os endereços IP obtidos para todas as placas de rede do computador.
/renew	Renova um endereço IP obtido para uma placa de através de um servidor DHCP. Se a placa de rede não for especificada, renova os endereços IP obtidos para todas as placas de rede instaladas no computador.
adaptador	Especifica uma placa de rede na renovação ou liberação de um endereço IP obtido através de um servidor DHCP. Para saber os nomes associados às placas de rede, utilize o comando Ipconfig sem parâmetros.

Nbtstat

Exibe estatísticas de protocolos e conexões TCP/IP usando NetBIOS sobre TCP/IP.

nbtstat [**-a** *hostname*] [**-A** *endereço IP*] [**-c**] [**-n**] [**-R**] [**-r**] [**-RR**] [**-S**] [**-s**] [*intervalo*] [-?]

Opção	**Descrição**
-a	Exibe a tabela de nomes NetBIOS registrados em um computador (determinado pelo *hostname*).
-A	Exibe a tabela de nomes NetBIOS registrados em um computador remoto (determinado pelo endereço IP).
-c	Exibe a lista de nomes NetBIOS (e endereços IP) do cache NetBIOS do computador.
-C	Exibe a lista de nomes NetBIOS (e endereços IP) do cache NetBIOS do computador para cada placa de rede.
-n	Exibe os nomes NetBIOS e os serviços registrados no computador local.
-r	Exibe os nomes NetBIOS resolvidos através de WINS ou mensagens *broadcast*.
-R	Recarrega o cache de nomes NetBIOS utilizando as entradas no arquivo LMHOSTS com o parâmetro #PRE.
-RR	Envia pacotes de liberação de nomes ao WINS e atualiza a lista de nomes.
-s	Exibe as sessões TCP/IP estabelecidas no computador (usando nomes de host do arquivo HOSTS).
-S	Exibe as sessões TCP/IP estabelecidas no computador (usando endereços IP).

intervalo Especifica o tempo (em segundos) de pausa intermediária para reexibir as informações selecionadas. Pressione Ctrl+C para interromper a exibição.

Ping

```
Prompt do MS-DOS

C:\WINDOWS>ping ederson

Disparando contra ederson [169.254.178.132] com 32 bytes de dados:

Resposta de 169.254.178.132:bytes=32 tempo<10ms Tempo de vida=128
Resposta de 169.254.178.132:bytes=32 tempo<10ms Tempo de vida=128
Resposta de 169.254.178.132:bytes=32 tempo<10ms Tempo de vida=128
Resposta de 169.254.178.132:bytes=32 tempo<10ms Tempo de vida=128

Estatísticas do Ping para 169.254.178.132:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Tempos aproximados de ida e volta em milissegundos:
    Mínimo = 0ms, Máximo =  0ms, Média =  0ms

C:\WINDOWS>
```

Utilizado para testar a conexão com outro host. O Ping envia uma mensagem ao host remoto e aguarda uma resposta contendo a mesma mensagem (*echo*). Se essa resposta chegar, presume-se que o host esteja vivo (literalmente).

ping *endereçoIP* | *hostname* [*chaves*]

Opção	**Descrição**
endereçoIP	Endereço IP (ou hostname) do host com o qual se está testando a conexão.
-a	Realiza a resolução DNS reversa, informando o hostname do host.
-n número	Define o número de comandos Ping que serão executados.
-l tamanho	Define o tamanho da mensagem utilizada no comando Ping (default=32 bytes).
-f	Define a flag; "Do Not Fragment" – envia a mensagem sem fragmentá-la.
-i *ttl*	*Time To Live* – Define o máximo número de *hops* pelos quais os pacotes podem passar (1-255).
-j *hosts*	Rota de origem livre usando as entradas em *hosts*.
-k *hosts*	Rota de origem restrita usando as entradas em *hosts*.
-r *número*	Registra a rota dos pacotes. Define quantos *hops* serão armazenados (máximo=9).
-s *número*	*Timestamp* do número de *hops* especificado.
-v TOS	Especifica o tipo de serviço a ser utilizado.
-t	Emite comandos Ping continuamente até ser interrompido. Normalmente Ctrl+C é utilizado para interromper.

-w Define o tempo máximo que o comando aguardará por uma resposta (*timeout*).

Alguns roteadores, por questões de segurança, não encaminham pacotes enviados através do protocolo ICMP (utilizado pelo Ping). O comando Ping pode não obter sucesso devido a essa *filtragem*.

Telnet

Conecta-se a uma máquina remota , utilizando seus recursos disponíveis.

telnet [*host* [*porta*]]

Opção	Descrição
host	Nome de host ou endereço IP do endereço remoto.
porta	Endereço da porta remota.

Comandos Interativos do Telnet

close	Fecha uma conexão.
display	Exibe opções de conexão.
environ	Define variáveis de ambiente.
logout	Encerra uma conexão.
mode	Alterna entre o modo de transferência ASCII e binário.
open	Efetua a conexão com um computador remoto.

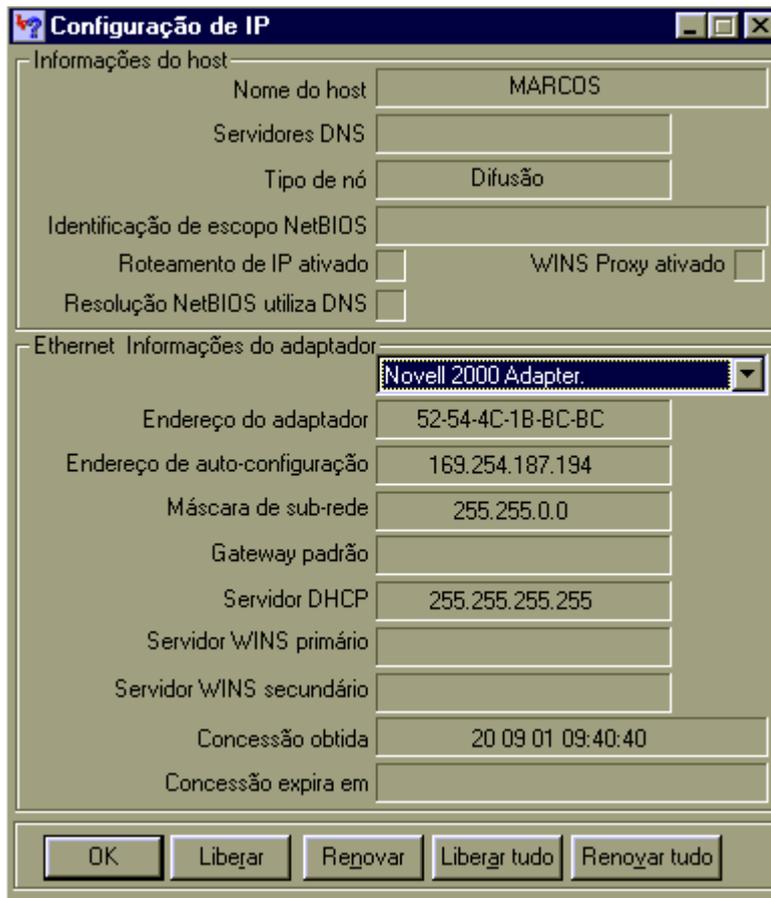
quit	Sai do Telnet.
send	Envia seqüências de protocolo Telnet especiais para um computador remoto.
set	Define opções de conexão.
unset	Desativa parâmetros de conexão.

Tracert

O Tracert (traçar rota) serve para verificarmos quantos e quais computadores os nossos dados passam até chegar a um destino especificado. No exemplo acima, levou apenas um computador para alcançar o destino pedido.

tracert [**-d**] [**h-** *hopsmáx*] [**-j** *listahops*] [**-w** *timeout*] *destino*

Opção	**Descrição**
-d	Não converte os endereços em nomes de host.
-h	Número máximo de *hops* (TTL) para encontrar o destino.
-j	Rota de origem livre com a *listahops*.
-w	*Timeou*t, ou tempo máximo para resposta (em milissegundos).
destino	Nome do host de destino (ou endereço IP).

Winipcfg

O Winipcfg é uma excelente ferramenta no que se trata de mostrar informações sobre o protocolo IP. Podemos dizer que ele é o IPCONFIG com interface GUI (digamos, bonitinha). Ele lhe mostra seu IP local, IP da rede, máscara da sub-rede e muito mais. Para acessá-lo, vá em iniciar / executar e digite winipcfg.

5

Footprinting

Footprinting é a arte de obter informações sobre um sistema alvo usando táticas “seguras”, sem perigo de detecção, e que pode dar muitas informações sobre ele. Tais como visitar o site da empresa em que se quer invadir e ler as seções para ver se encontra algo de interessante.

Whois

O Whois é excelente para obtermos informações sobre sites. Bancos de dados como o Internic (www.internic.org) mantêm informações interessantes sobre os domínios, tais como nome do dono, endereço e telefone. No Brasil, o orgão responsável por essa tarefa é a Fapesp e podem ser feitas pesquisas no seguinte endereço: www.registro.br.

Análise de homepages

Consiste em entrar no site , ler tudo quanto é página, homepages pessoais de funcionários (se for uma empresa), absolutamente tudo. Parece incrível mas muitos lugares mostram até configurações da rede em suas páginas. O código em html também deve ser analisado a procura de comentários. Muitos deles podem ser extremamente úteis. Cheque todos os links, observe os endereços em que as páginas se posicionam. Já dá para começarmos o montar um mapa da rede (antes de fazer um ataque direto scanneando mais tarde).

Pesquisa geral

Use ferramentas de busca como o Altavista para descobrir outras páginas com o nome do domínio atacado. Pesquise em jornais notícias em jornais e revistas sobre o "inimigo" , tais como se ele já foi atacado, se já sofreu algum tipo de invasão, etc. Tente conhecer pessoas que trabalham lá , ter uma noção de quantos empregados existem tomando conta daquele servidor. Enfim, quanto mais você puder descobrir na pesquisa geral, mas fácil o seu trabalho ficará depois.

Ferramentas e segredos

6

Trojans

Definição de Trojan

O nome trojan é uma alusão à história do antigo cavalo de tróia, em que o governante da cidade de Tróia na antiga Grécia foi presenteado com um cavalo de madeira no qual havia escondido soldados inimigos. Possui muitas características similares aos vírus, tais como: perda de arquivos, falhas na memória, erros em periféricos, etc... A grande diferença é que o trojan pode ser considerado um vírus inteligente, pois é controlado à distância pela pessoa que o instalou. Esse indivíduo então, consegue "enxergar" o seu computador, podendo realizar desde as mais simples tarefas como mexer o mouse à utilização do seu IP como ponte para outros ataques. Conseguem ficar escondidos em arquivos de inicialização do sistema operacional e se iniciam toda vez que a máquina é ligada.

Perigo real

A popularização da Internet e a facilidade de se criar um programa cavalo de tróia fazem com que esse método de invasão seja atualmente o mais perigoso de todos. Ele não depende de falhas no seu sistema, é quase indetectável e pela sua facilidade de uso pode ser operado por crianças de 6 anos. Pode-se esconder um trojan em fotos, arquivos de música, aplicativos e jogos. Sendo assim, nunca abra arquivos executáveis enviados por estranhos ou pegos em sites duvidosos. Existem muitas técnicas para se instalar um trojan em uma máquina. Um bom exemplo no Windows 98/ME é mapeando a unidade desse computador (netbios), copiar o programa e alterar o arquivo win.ini Assim toda vez que você for jogar paciência ou mesmo abrir o bloco de notas, tome cuidado com o tamanho do arquivo executável. Se estiver muito grande, desconfie.

Tipos de cavalo de tróia

Invasão por portas TCP e UDP

Esse é o trojan mais comum existente na Internet hoje. Netbus, Back Orifice, SubSeven, Hack'a'tack, Girlfriend, Netsphere e muitos outros são facilmente encontrados pela rede. Possuem na sua maioria dois arquivos: um servidor para ser instalado no computador da vítima e um cliente com interface gráfica para manipular o servidor remotamente. As portas de um sistema variam entre 0 e 65535 e servem para identificar serviços rodando no sistema(como o servidor web que utiliza a porta 80). O servidor se torna mais um serviço ao escolher alguma porta para "escutar" as chamadas do cliente.O trojan que utiliza portas TCP, estabelece uma conexão com o servidor, atuando diretamente de dentro do sistema. Já o que

utiliza portas UDP, comunica-se via pacotes de dados enviados ao host alvo. Não tão confiável como o TCP, não garante a entrega dos pacotes e o recebimento da resposta. Quase todos os trojans atuais são para a arquitetura Windows. Os poucos existentes em outros sistemas, tais como: Unix, Linux, Novell e Macintosh são chamados de *backdoors*. A diferença entre o trojan comum e o backdoor é que o último é muito mais difícil de se instalar. Em um sistema Unix por exemplo, para conseguir se instalar um backdoor é preciso possuir privilégios de super usuário (root).

Trojans de informação

Não é tão usado quanto o de portas mas igualmente (ou até mais) perigoso. Enquanto a maioria das funções dos trojans comuns é apenas para aborrecer(sumir com a barra de tarefas, apagar o monitor, desligar o Windows, etc...), o trojan de informação se concentra em ficar residente detectando todos os tipos de dados vitais do sistema. Ele consegue toda senha digitada no servidor junto ao endereço ip das máquinas e envia a informação para uma conta de e-mail configurada pelo invasor. Existem alguns programas mais sofisticados que além de enviar por e-mail, pode enviar a informação por icq ou qualquer outro tipo de messenger. Geralmente o programa envia a informação em um prazo de cada 5 a 10 minutos. Ao contrário do trojan de portas, possui apenas o arquivo servidor e um tamanho bem menor. Exemplo: o servidor do trojan de portas **Netbus** possui cerca de 490 kb de tamanho. Já o trojan de informações **k2ps** possui cerca de 17 kb.

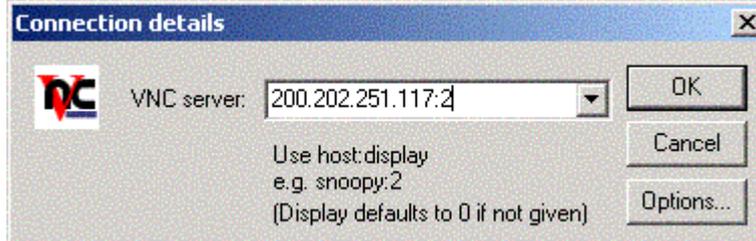
Trojans de ponte

É um tipo não muito conhecido mas largamente usado por hackers e crackers do mundo inteiro. Consiste em instalar um servidor no seu computador que possibilite que através dele (e do seu endereço ip) o invasor possa realizar ataques de invasão e de recusa de serviço. Então, se um grande site for invadido e baterem na sua casa, procure pois deve haver algum desses no seu sistema. Um programa comum é o WinProxy, que pode ser instalado facilmente e não levanta nenhum tipo de suspeitas. Conheço alguém que o possui na sua máquina e jura que é um firewall. Leia mais sobre os trojans de ponte na seção *anonimidade*.

Rootkits

Esse tipo especial de backdoor é utilizado no Unix e Linux. Ao ser executado pelo operador do sistema ele substitui arquivos executáveis importantes (como o ps por exemplo) por versões "infectadas". Essas versões podem ser tanto trojans de portas quanto de informação. Vão fornecer acesso irrestrito ao invasor com poderes de super-usuário, e o mais importante: os acessos não ficam registrados nos logs. Para conhecer alguns dos rootkits mais usados e o tipo de alteração causada por eles, visite o website: **www.rootshell.com.**

Trojans comerciais

Alguém já ouviu falar do PcAnywhere? Ou do terminal remoto do Windows 2000 e XP? Esses programas (além de muitos outros) possibilitam que você controle completamente a máquina de alguém, como se estivesse sentado ali. Quer jogar Quake no computador invadido? Clique no botão iniciar dele e faça tudo como se estivesse no seu próprio computador. A vantagem desses programas (já que são comerciais), é que o anti-vírus não pega. Tente também o excelente VNC (que pode ser pego em www.superdownloads.com.br), que é gratuito. Se você configurar direitinho um programa desses na vítima, seja piedoso.

Cliente para conexões do programa comercial VNC, criado pela AT&T

Escondendo o trojan em arquivos confiáveis

Existem muitos programas na Internet que escondem os servidores em arquivos executáveis. Um deles é o **The Joiner**, que possibilita você juntar o trojan com algum outro executável e criar um terceiro contendo os dois. Além de possibilitar que o coloque em fotos. Um método engraçado muito utilizado hoje pelos que se dizem "hackers", é renomear algum executável para foto e deixar um largo espaço. Por exemplo: supondo que o nosso servidor é o arquivo **server.exe.** Então iríamos renomeá-lo para **loira.jpg   .exe.**

Assim muitos usuários inexperientes caem no truque. Todos os métodos citados anteriormente têm somente uma falha: se você criar um executável pelo The Joiner ou renomear o servidor, qualquer programa anti-vírus logo detectará o arquivo. Para que o anti-vírus não o detecte, é só usar a imaginação. Crie um programa em alguma linguagem e coloque o servidor no meio dos arquivos. Faça com que o programa quando executado renomeie o servidor e o execute. Assim, se o servidor estiver como **voodoo.dll** passe-o para **sysconf.exe** e execute. Esse método não é infalível mas engana a grande maioria dos programas de detecção. Mas não todos. Anti-vírus geralmente o pega.

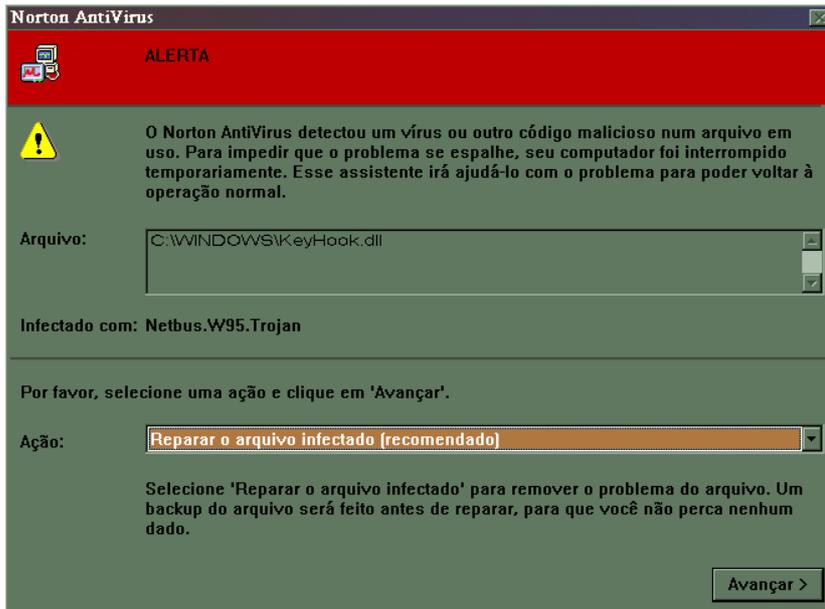
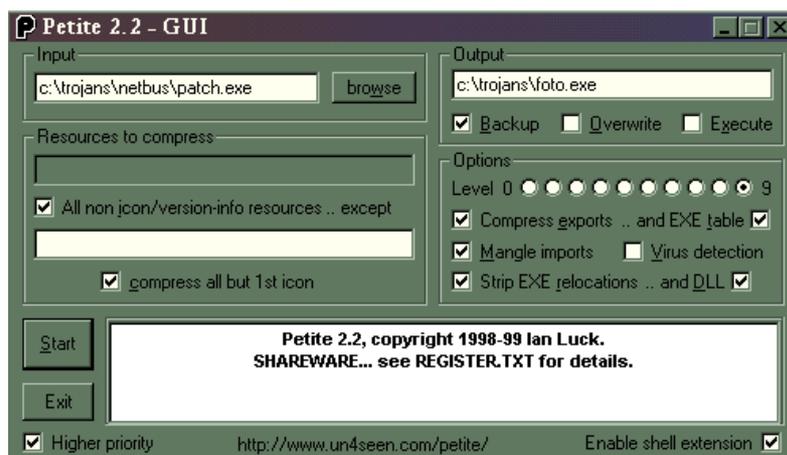
The Joiner: esconda o servidor em outro arquivo

Utilizando compressores de executáveis

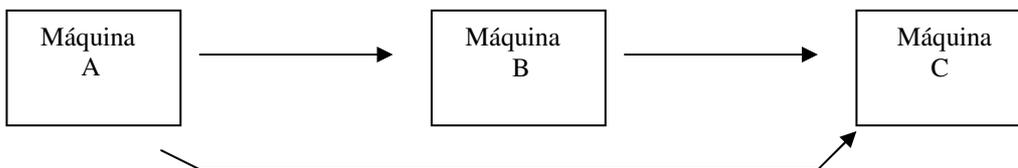
Como vimos no ítem anterior, vários métodos podem ser usados para esconder um cavalo de tróia. Depende mais da imaginação do invasor. Só que ainda assim podem ser facilmente detectados. Esse é o primeiro livro a citar o método do compressor de executáveis windows 32 bits, apesar de essa técnica já vir sendo utilizada em larga escala. Consiste em usar um programa compressor de arquivos EXE, que apenas diminua o seu tamanho retirando espaços vazios desnecessários. Um programa comum é o **Petite** que diminui cerca de 30% ou mais do arquivo original. Um trojan (ou mesmo um vírus) comprimido é absolutamente indetectável por anti-vírus e scanners. Isso porquê esses programas se baseiam na estrutura do arquivo para identificá-lo. É como se tivesse fotos na memória e as comparasse. Como não encontrou

nenhuma igual, não mostra nenhum tipo de aviso. Um operador de sistemas têm que conhecer muito bem seus arquivos e conferir sempre novas alterações (como datas e horas de novos arquivos) para evitar que um trojan comprimido seja instalado em seu sistema. Não dependa só de anti-vírus. Mas atenção: os compressores de executáveis não comprimem arquivos que já foram comprimidos (como o server do trojan subseven).

Vamos realizar passo a passo o processo de esconder um trojan de um anti-vírus.

1. **Passaremos o Norton para que encontre o arquivo infectado:**

2. **Agora, abriremos o programa PETITE para comprimir o arquivo EXE do servidor do Netbus.**

3. **Com o arquivo já comprimido, novamente testamos o anti-vírus**:

Spoofando uma porta

É muito raro a utilização do spoof em trojans. Isso porquê se a pessoa envia um pedido de conexão a um servidor, ela precisa estar usando o seu endereço IP real para receber a resposta. Apenas com o protocolo UDP, que envia comandos sem estabelecimento de conexão, isso é possível. Em quase todos os casos, o endereço IP capturado por um programa anti-trojans é realmente o do invasor. A única exceção é quando se utiliza um trojan de ponte para se conectar a outro (geralmente TCP). Exemplo:

A **máquina A** têm duas opções. Pode se conectar ao trojan existente na **máquina C**. Mas o invasor não quer correr nenhum risco pois não está usando nenhum tipo de recursos de anonimidade. Então ele se conecta à **máquina B** que está na mesma rede que a **máquina C** mas não possui nenhum tipo de segurança. Se utilizando da confiança entre as duas máquinas, ele se conecta à **máquina C** que vai responder tudo o que invasor quiser, pois pensa que é a **máquina B**. Essa técnica, chamada de IP Spoof, foi utilizado pelo hacker Kevin Mitnick para conseguir acesso ao computador do analista de sistemas Shimomura. O processo será descrito em detalhes na seção anonimidade.

Métodos eficazes e os não tão eficazes de se retirar o programa

Basicamente existem quatro métodos de se retirar um cavalo de tróia. Cada um possui suas vantagens e falhas. O ideal seria usar um pouco de todos.

Detecção por portas

Esse é um método utilizado por programas como o **Xôbobus,** o meu **Anti-Trojans** e muitos outros**.** Funciona do seguinte modo: os programadores estudam as portas TCP e UDP utilizadas pelos trojans e criam um programa que abre essas portas. Assim, quando um invasor vir a porta aberta e pensar que é um cavalo de tróia que está instalado ali, cairá em uma armadilha tendo o seu endereço IP detectado. Esse método não é muito eficiente pois facilmente podemos mudar as portas que os trojans utilizam. Mas ainda é um método muito usado pois muitas pessoas não se lembrar de trocar as portas.

Detecção pelo arquivo

Esse é o método usado pelos anti-vírus e o programa The Cleaner. Ele detecta o trojan checando a sua estrutura. Se o arquivo estiver renomeado (sem ser para executável) ou estiver comprimido, esse método se torna inútil. Para ser realmente eficaz, deve ser usado junto à detecção de portas. Assim, mesmo que seu anti-vírus não encontrou um trojan, o Anti-Trojans pode encontrar.

Detecção por string

Na minha opinião, o melhor método de todos. Pouco divulgado publicamente, se torna a melhor garantia para se detectar um trojan sem falhas. Isso porquê mesmo que o programa for comprimido ou mude suas portas, ele ainda estará usando uma das 65535 portas do sistema e se comunicará com o cliente. A comunicação entre cliente e servidor se dá por uma string (texto) enviada. Por exemplo: O **Netbus 1.7** envia uma string assim “Netbus 1.7x” quando alguma conexão é estabelecida. Se for o cliente, ele responderá com outra string. Então para analisar todas as portas do seu sistema e saber quais estão abertas e possuem strings, utilize um programa como o **Chaoscan** ou algum outro scanner de porta que lhe dê essas informações.

Detecção manual

Muito eficaz também, a checagem manual do sistema pelo operador pode facilitar muito a vida. Olhando registro, arquivos de inicialização, conferindo os programas carregados na memória, o tamanho dos arquivos, etc... Todas essas precauções evitam dores de cabeça. Essa política adotada junto aos outros tipos de detecção faz com que você exclua em 100% a chance de uma invasão por cavalos de tróia.

Passo-a-passo: cavalos de tróia

Utilizando um trojan

Vamos utilizar um trojan para nos conectarmos a algum computador infectado. Antes de tudo, verifique se o computador alvo está com o servidor instalado (o arquivo que comprimimos anteriormente). Agora seguiremos os seguintes passos com o trojan Netbus:

1. Abra o programa Netbus (se o anti-vírus acusar vírus, passe o petite nele também)
2. Em hostname / IP , coloque o IP da máquina a ser invadida (se for seu próprio computador, utilize 127.0.0.1). Se a porta no servidor for diferente de 12345 (o padrão do Netbus), coloque-a em port.

3. Clique em connect!

Ao aparecer a mensagem "**Connected**" na barra de status, significa que a invasão foi bem sucedida. Vamos agora realizar algumas ações:

1. Clique em Open CD-ROM para abrir o drive de cd da vítima.
2. Vá em Start Program e coloque **c:\windows\calc.exe** para abrir a calculadora.
3. Clique em Go to URL e mande a pessoa para algum site.
4. Use Listen para pegar os caracteres digitados pela pessoa e intervir no meio (como se você estivesse escrevendo no Word e de repente as palavras se formam sozinhas).
5. A Port Redirect cria uma ponte. Coloque uma porta (geralmente use a 80) e um site. Assim quando for ao Internet Explorer e digitar o IP do computador invadido, você cairá nesse site configurado. Por exemplo: ao digitar **127.0.0.1** no browser fui enviado para **www.whitehouse.gov**.
6. Dá para fuçar bem nas opções, mas a mais interessante é a App Redirect. Abra-a, coloque uma porta qualquer (100 por exemplo) e mande executar um shell nessa porta (no caso do Windows 95, 98 e ME, use **c:\command.com** , no NT, 2000 e XP use cmd.exe). Agora utilize o **telnet** (vá em iniciar/ executar e digite: telnet 127.0.0.1 100 , trocando o endereço ip padrão pelo da vítima) e pronto. Você está no prompt do MS-DOS da pessoa. Têm o controle total da máquina.
7. Para desconectar, apenas clique em disconnect.
8. A opção server admin retira o servidor.

Utilizando o Anti-Trojans

Vamos utilizar como exemplo de detecção por portas, o meu programa **Anti-Trojans** versão 1.6. Se quiser tentar outro programa, tente o Xô Bo Bus brasileiro ou algum estrangeiro (procure no Superdownloads). É claro que um firewall (como veremos depois) é mais potente. Mas é mais complicado para usuários comuns. Veremos passo a passo.

1. Abra o programa

2. Clique na pasta Configuração , e coloque a mensagem para a pessoa que tentar lhe invadir. Se quiser, configure um e-mail para que a tentativa de invasão seja reportada.
3. Clique na pasta Monitorar.
4. Clique no botão Monitorar. Agora clique com o botão direito no ícone do superman na barra de tarefas e selecione esconder.
5. Simule uma tentativa de invasão indo em Iniciar / Executar e digitando:

telnet 127.0.0.1 12345

O programa irá detectar a tentativa de invasão e mostrará uma mensagem com o horário, o endereço IP do invasor, o seu host e o tipo de invasão tentada.

Para terminar o capítulo de trojans, uma pequena dica: altere o arquivo autorun.inf de algum cd (aquele que faz o cd rodar sozinho quando no drive) e faça-o executar algum servidor. É simples, até com o bloco de notas dá para fazer a alteração. Daí é só gravar o cd (em uma gravadora, com alguns outros programas para despistar) e pronto. Quem desconfiará de colocar um simples cd no drive? Esse processo também funciona na unidade C e em disquetes. Experimente!

7

Denial of Service

Definição

A diferença entre um cracker e um script kiddie pode ser vista aqui. Um invasor decente estuda em detalhes o sistema alvo, às vezes por meses, conhecendo todo o seu processo de autenticação, usuários e falhas que podem levá-lo a ter acesso a arquivos vitais. Já o script kiddie pega algum programinha de alguma homepage duvidável de fundo preto e imagens de caveiras animadas, tenta usá-lo no primeiro sistema que vê na frente e se não consegue invadí-lo , o derruba para mostrar que é "bom". Isso é absolutamente inútil, afinal se o sistema travar e cair devido ao Denial of Service, provavelmente ele volta a funcionar com questão de poucos minutos. Ou o administrador competente rapidamente percebe. Alguns programas bons para essa tarefa são o **Agressor,** o **IGMP Nuker** e o **Divine Intervention** (para Windows). Para Linux e Unix, sem dúvida o melhor é o excelente **Tribal Flood Network**.

Danos sem invasões

Por ser um ataque apenas voltado para o consumo de memória ou do processamento, o DoS não é usado para invasão. Ao contrário de alguns programas que causam um estouro de memória já sabendo que esse problema lhe dará acesso ao sistema (programas que causam buffer overflow), a intenção do DoS é só chatear. Mesmo assim em grandes empresas o prejuízo pode ser grande. Quando a *Amazon.com* foi tirada do ar por exemplo, chegou a ficar apenas poucos minutos desligada, mas nesse tempo perdeu muito dinheiro em compras. O mesmo aconteceu com o Yahoo e até com o UOL, que já foi tirado do ar.

Utilizando o broadcast como arma

Realizar um ataque de DoS é muito simples. Pode-se utilizar vários tipos de programas e softwares zumbis para fazê-lo. Às vezes nem é preciso um programa adicional. Sites como Yahoo e Altavista utilizam **webspiders** (programa utilizado para procurar informações pulando de link em link) para checar o conteúdo de homepages. Muitos webspiders checando o mesmo servidor ao mesmo tempo pode levá-lo ao colapso. Causar um DoS em algum servidor de e-mail é ainda mais fácil. Utilizando um programa de **e-mail bomba** (software que envia milhares de e-mails para o mesmo endereço) ou cadastrando o e-mail alvo em serviços de spam (como mensagens de anjos, piadas, notícias e outros) pode encher a sua caixa postal e travar todo o sistema. Ou mande um e-mail para alguém que tenha serviço de resposta automática , utilizando o próprio endereço da pessoa. É assim: mande uma mensagem para **fulano@provedor.com.br** usando esse e-mail (como se fosse o seu, já que

pra mandar e-mails não se precisa de senha). A resposta automática da caixa postal do Fulano mandará mensagens para ele mesmo, travando sua caixa postal. O endereço de broadcast de redes geralmente é o com final 255 (exemplo: 200.202.243.255). A solução para o problema do e-mail é mais simples. Apenas use um bom filtro ou algum programa que impossibilite que se receba mais de três e-mails enviados da mesma origem (endereço IP) durante um certo intervalo de tempo.

Uma tela de um programa e-mail bomba

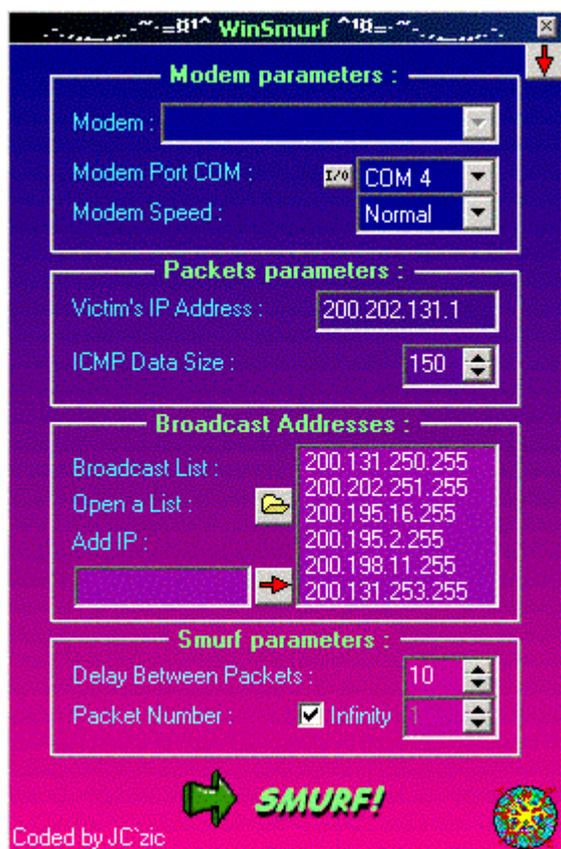
Syn-flood

O tipo de ataque usado para gerar o ip spoof. A autenticação por Syn é feita em três vias. O ataque consiste em não completar essas três vias. Mais ou menos assim. No caso do ping, ele é em duas vias, apenas envia o pacote e recebe a resposta. Para o Syn-flood, primeiro é enviado o pacote Syn e logo depois teria que ser enviado o Ack para a conexão se estabelecer, mas ele não é enviado, fazendo com que a máquina alvo consuma seus recursos ao receber muitos Syns e esperar muitos Acks. O ataque por ping é parecido, é enviado vários pings com grandes pacotes fazendo com que um sistema trave. Mas é mais difícil de ocorrer o travamento do que o ataque por syn.

OOB

Ataque Out-of-Band ou popularmente conhecido como WinNuke. Consiste em mandar pacotes malformados para uma porta Netbios do Windows. Geralmente usado nas portas 135, 137 e 139, essa última sendo a mais usada. O sistema não consegue lidar com os pacotes, trava e mostra a famosa tela azul de erro. No Windows 95 esse ataque era mais eficaz, agora está se tornando obsoleto.

Smurf

Na minha opinião o mais devastador de todos os ataques. Envia pacotes ICMP (protocolo que informa condições de erro) spoofados para centenas, talvez milhares de sites. Envia-se os pacotes com o endereço IP da vítima, assim fazendo com que ela receba muitos pacotes ping de resposta ao mesmo tempo, causando um travamento total. Ainda não existe uma proteção eficaz contra esse tipo de ataque. Um programa bom (para Windows) que realiza o smurf é o WinSmurf.

De azul e bonitinho esse smurf não têm nada.

Softwares Zumbis

Programas que automatizam o processo de causar um DoS em alguma máquina. São instalados em computadores estratégicos (como universidades, centros de pesquisa e outros) que possuem conexão rápida à Internet e configurados para atacar ao mesmo tempo. Se eu instalar o programa em vinte máquinas de diferentes endereços e configurá-las para enviar 10.000 pacotes cada uma, com certeza derruba qualquer host. Um programa muito utilizado para isso é o **Tribal Flood Network**. Trojans também são largamente usados para esse fim.

Diminuindo o impacto causado pelos ataques

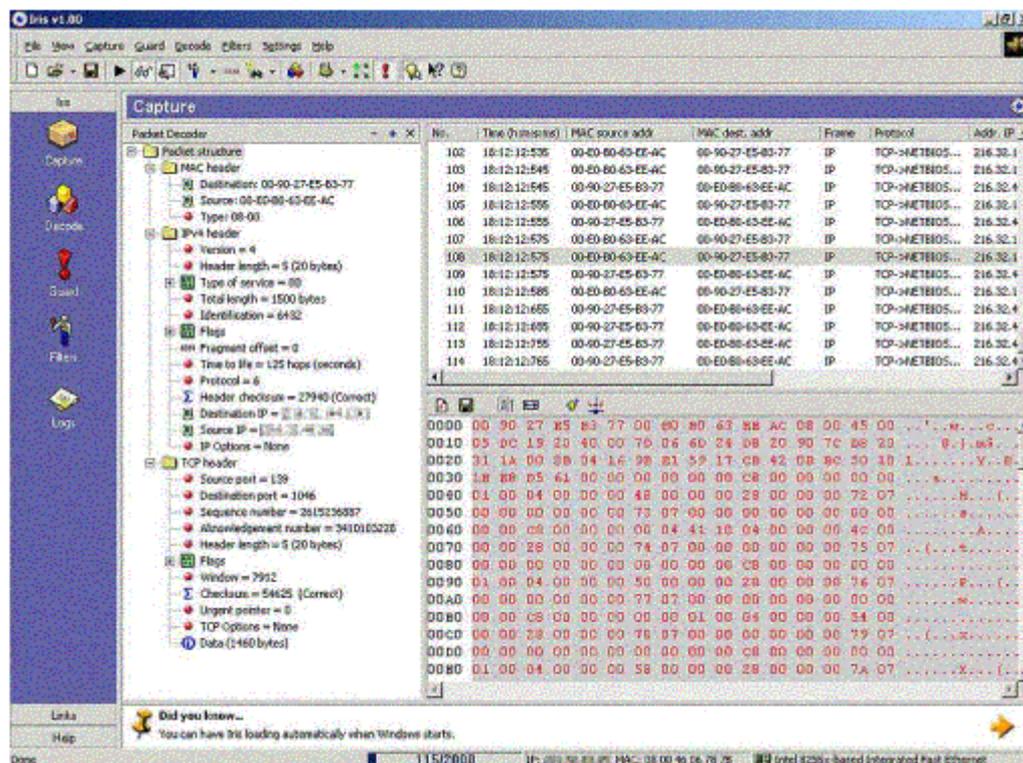
O melhor procedimento para se adotar é procurar os sites do fabricante do sistema operacional e pegar atualizações para as falhas. Como é o caso do OOB(Winnuke). A Microsoft já colocou um patch de correção em sua homepage. Evitar o máximo de uso desnecessário da memória, assim dificultando um pouco os ataques. E sempre que puder,

aumentar a capacidade de processamento e a memória RAM do sistema. Isso não vai impedir os ataques pois alguns não têm solução, mas só funcionam mesmo quando utilizados em larga escala. O Smurf por exemplo, para derrubar um computador pessoal é fácil, mas um grande host para cair seria preciso muitas pessoas realizando o ataque ao mesmo tempo. Ou a utilização do software zumbi. A não ser que tenha comprado briga com alguns crackers, pode ficar tranqüilo.

8

Sniffers

Definição

Os sniffers ou farejadores são o tipo de programas mais usados para conseguir senhas em uma rede. Eles ficam residentes na memória como um cavalo de tróia, analisando todo o tráfego que ali passa. Qualquer entrada ou saída de dados é capturada, seja em um servidor FTP, uma página de chat ou um e-mail digitado. O sniffer pega os pacotes recebidos em seu estado bruto e os transforma em texto puro para serem lidos. Sempre foram mais usados em sistemas Unix, mas ultimamente todos os outros sistemas contam com poderosos sniffers. Desde sniffers comercias como o excelente Íris até sniffers mais simples, como o tcpdump e sniffers de trojans. Vamos fazer uma análise de como esses perigosos programas funciona.

Exemplo de uma tela de sniffer (programa IRIS)

Filtrando pacotes na rede

Muitas pessoas pensam que o sniffer pode ser usado em seu computador para capturar pacotes do seu provedor. Não é bem assim. O programa têm de estar instalado no computador central de uma rede em que se quer capturar pacotes. Utilizando o exemplo do provedor, todos os seus usuários realizam o processo de autenticação em um servidor antes de conectarem-se à rede. Assim, primeiro é necessário conseguir invadir o servidor e depois colocar o sniffer. Ele irá monitorar absolutamente tudo, às vezes até informações pessoais dos usuários, como endereço e telefone. Como são muitos os pacotes em uma rede, o farejador é configurado para obter somente o essencial e importante: as senhas.

Capturando senhas

A principal preocupação de um operador é , ou pelo menos deveria ser, as senhas. Afinal, por mais seguro que o sistema seja, uma senha adquirida maliciosamente é sempre perigosa. O único interesse dos crackers é capturar logins e senhas. Nem se encontrar um e-mail de sua namorada para o amante o cracker deixará de se concentrar em sua tarefa. Existem algumas opções que ainda possibilitam filtrar os tipos de pacotes recebidos. Vamos supor que eu quero descobrir todas as senhas que comecem com "C". Após configurar o sniffer e esperar, ele começa a me enviar os pacotes recebidos já "selecionados" com o que desejo.

Sniffers em trojans

Alguns trojans como o **Back Orifice** possuem sniffers como plug-ins (partes extras que podem ser anexadas ao programa). O **Buttsniffer**, um dos melhores plug-ins para o BO monitora absolutamente tudo no sistema Windows. Além de ter um arquivo executável à parte, podendo funcionar sem depender do Back Orifice. Alguns outros trojans mais novos já possuem o sniffer embutido. A tendência do sniffer e do trojan é de se tornarem uma ferramente apenas, já que ambos têm características parecidas. O trojan de e-mail **k2ps** é um bom exemplo disso. Ele monitora e envia todo tipo de senha importante por e-mail (na verdade, alguns o consideram um keylogger que é um programa que loga tudo que se escreve no teclado, eu não o considero assim pois ele é seletivo: só envia coisas importantes).

Roteadores

Alguns sniffers conseguem obter dados direto do roteador. Mesmo que seja instalada uma proteção eficaz no sistema operacional, como um anti-sniffer, não adiantaria de nada se o programa estiver pegando os dados diretamente roteados. A correção têm de ser feita atualizando-se o próprio roteador. O ideal seria procurar a página do fabricante e verificar se existe alguma dica ou informação sobre o assunto. Afinal, o seguro morreu de velho.

Anti-Sniffers

Como o próprio nome diz, são programas que detectam tentativas de sniffing. Ficam residentes na memória como um anti-trojans, aguardando o invasor tentar algo. Há vários tipos de anti-sniffers, alguns bem ruinzinhos e outros muito bons. Uma boa opçãos do software são fingir o envio de dados, para que o cracker engane-se e pense que realmente está conseguindo as senhas. Se você têm sofrido muitas invasões, certificou-se de não ser por falhas ou trojans, monte um **honeypot** com um anti-sniffer. Com certeza deve pegar alguma abelhinha. Experimente o programa Anti-sniff que pode ser pego no Superdowloads (www.superdownloads.com.br).

9

Scanners

Definição

Todos sabemos que nenhum sistema é perfeito. Falhas em programas e sistemas existem sim e são uma ameaça à segurança. Geralmente ocorre do seguinte modo: um administrador acidentalmente descobre que algum recurso do seu sistema gera um erro em resposta a algum tipo de pedido. Para exemplificar, suponhamos que a rede em que o administrador trabalha só se comunica gerando mensagens de "olá". Um dia ele escreve "alô" sem querer e descobre que ao enviar a mensagem para outra máquina, ela fica confusa e trava. Bem, a resposta deveria dizer "Desculpe, só olá aceito". Foi descoberto um **bug**. Agora imagine que centenas de bugs são descobertos a cada dia e que o seu sistema "confiável" de hoje, pode ser destruído amanhã. Existem algumas saídas para fazer uma análise mais garantida. A primeira é que você se torne um completo *nerd* e conheça desde o primeiro ao último bug existente. Se você trabalha com mais de um tipo de sistema operacional então, boa sorte. Uma outra saída, infinitamente mais eficaz, é a utilização de **scanners**. São programas que analisam um sistema ou rede em busca de falhas de qualquer tipo. Existem dezenas de scanners diferentes, cada um com suas vantagens. Aprendendo melhor sobre eles, poderá se proteger melhor e evitar que algum invasor malicioso dê um passo à sua frente.

Descobrindo falhas em um host

Para entender qual a parte do seu sistema é mais vulnerável, você terá que pensar com malícia. Ora, se você usa um firewall e desabilita o acesso externo aos servidores de FTP e Telnet, com certeza eles não serão a sua maior preocupação. Em alguns hosts , deixa-se habilitada apenas a porta 80 (www) para acesso externo. Muitos se sentem seguros desse modo. Mas enganam-se. Atualmente, a quantidade de falhas existentes em servidores World Wide Web é absurda. Tanto Internet Information Server quanto Apache ou qualquer outro, possuem erros. Alguns deles tão perigosas que possibilitam acesso ao interpretador de comandos do sistema, podendo gerar uma "entrada" para o invasor na rede. Outros podem fazer com que se consuma toda a memória existente, causando um *Buffer Overflow*(nome dado ao travamento do sistema devido a falhas de memória). Vamos dividir o nosso estudo sobre scanners em partes: os scanners de portas, scanners de host, scanners netbios e scanners de vulnerabilidade.

Portas abertas com serviços ativos

Ao contrário do que popularmente se pensa, não é tão fácil assim invadir um computador pessoal. Nós já sabemos que o sistema é composto de 65535 portas TCP e UDP. Em servidores, muitas delas possuem serviços rodando, tais como:

21 - FTP (File Transfer Protocol)

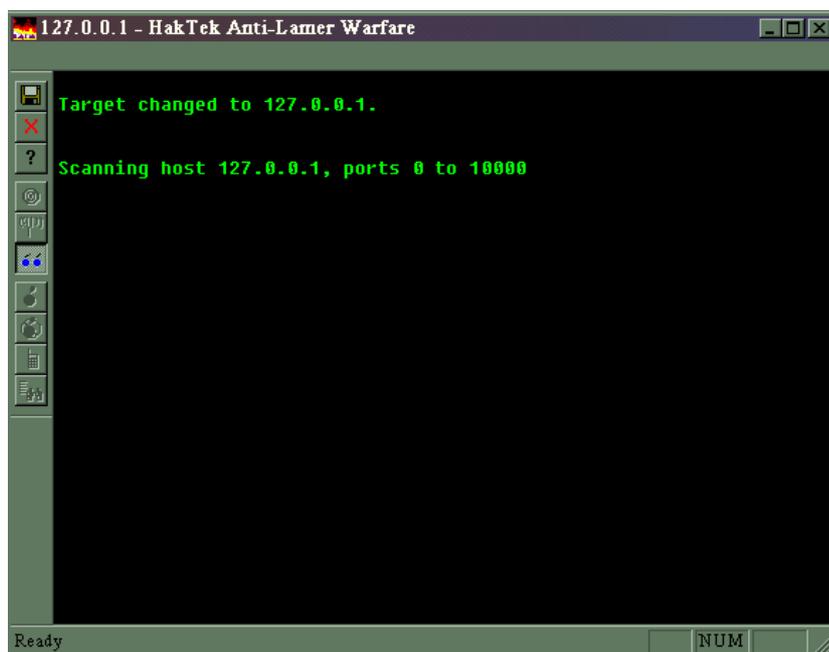
23 - TELNET

25 - SMTP (Simple Mail Transfer Protocol)

79 - FINGER

80 - WWW

Esses são apenas alguns dos muitos serviços que são rodados em computadores de empresas que precisam estabelecer contato com filiais e clientes. Realmente, um sistema que possua os seguintes serviços acima ativos, pode ganhar sérios problemas com segurança. Mas imagine o seu computador na sua casa, em cima da mesa da sala, cheio de joguinhos dos seus filhos e que você só utiliza para ler e-mails e navegar pelas homepages. As portas da sua máquina estão descansando totalmente. Às vezes, uma ou outra se abre para estabelecer conexão com um site, ou mandar uma mensagem pelo ICQ. Mas essas são **randômicas**, ou seja, a cada vez que uma conexão for feita, a porta mudará. Isso impede que algum invasor fique à espreita e tente se conectar a portas padrões. Dificulta, mas não impede. Algum cavalo de tróia instalado sem você saber pode abrir uma porta qualquer e permitir a conexão de qualquer pessoa. Para saber quais portas estão abertas em um sistema remoto, utilizamos o **scan de portas**. Existem muitos e muitos programas desse tipo. Alguns exemplos são o Cha0scan , o Shadow Scan e o Haktek.

Funcionam da seguinte maneira: vão tentar se conectar a todas as portas de um endereço ip fornecido, mostrando todas as portas encontradas "ativas" e o seu conteúdo. É uma boa táticas para encontrar cavalos de tróia sem depender de **anti-vírus**, já que todos usam portas. Exemplo: eu quero analisar o meu próprio computador para saber se têm alguma porta aberta.

Para isso, vou usar o HakTek. Então mando o programa tentar scannear portas no endereço **127.0.0.1**(o chamado endereço de *loopback*. Serve para quando você não está conectado na Internet e precisa utilizar algum programa de análise que precise de endereço IP). Encontrei as seguintes portas ativas:

80

1256

21554

31337

Ora, a primeira porta eu sei que é o servidor de páginas que rodo no meu pc. Mas e as outras três? A porta 1256 era a que o icq havia aberto na hora. As outras duas são portas de trojans que usei como teste. A porta 21554 é do trojan Girlfriend e a porta 31337 é do Back Orifice.

O único problema desse scan é que como ele foi feito nas três vias do tcp (syn, syn-ack, ack) pode ser facilmente detectado por sistemas IDS (detecção de intrusos). Uma boa saída é usar o **NMAP** , disponível tanto em Windows NT quanto Linux. Utilizando-o, você pode scannear portas de maneira furtiva, sem realizar as três vias do tcp. Ele possui muitas opções diferentes para scan de portas, experimente-as.

Máquinas ativas da subnet

O segundo tipo de scanner estudado, é o mais usado quando o objetivo do invasor é determinar todos os hosts ativos da subnet e saber seus nomes (DNS). Assim, vamos supor que o endereço principal de um provedor é **www.phela.com.br**. Usamos um **ping** qualquer, ou o próprio scanner, e descobrimos que o endereço ip é **200.205.215.37**. Agora vou utilizar o scanner de hosts para saber quais outras máquinas dessa rede estão ativas.

200.205.215.9 - diretoria.phela.com.br

200.205.215.34 - laboratorio.phela.com.br

200.205.215.35 - milho.phela.com.br

200.205.215.36 - gilmara.phela.com.br

200.205.215.37 - server.phela.com.br

200.205.215.65 - route.phela.com.br

Com isso conseguimos informações importantes do sistema. Sabemos por exemplo qual é o endereço do roteador, e onde deve ficar informações importantes. Se fosse um site de comércio eletrônico por exemplo, as chances de conseguir os dados era enorme, pois mesmo que o invasor não conseguisse acesso diretamente ao computador **200.205.215.37** (que pode inclusive ser um firewall) ele poderia se conectar a um outro IP da subnet e conseguir os dados a partir dele. Às vezes poderia haver algum backup perdido por aí. Alguns bons scanners de hosts são o **Shadow Scan** ,o **Haktek** e o **projeto r3x,** entre outros.. Claro que

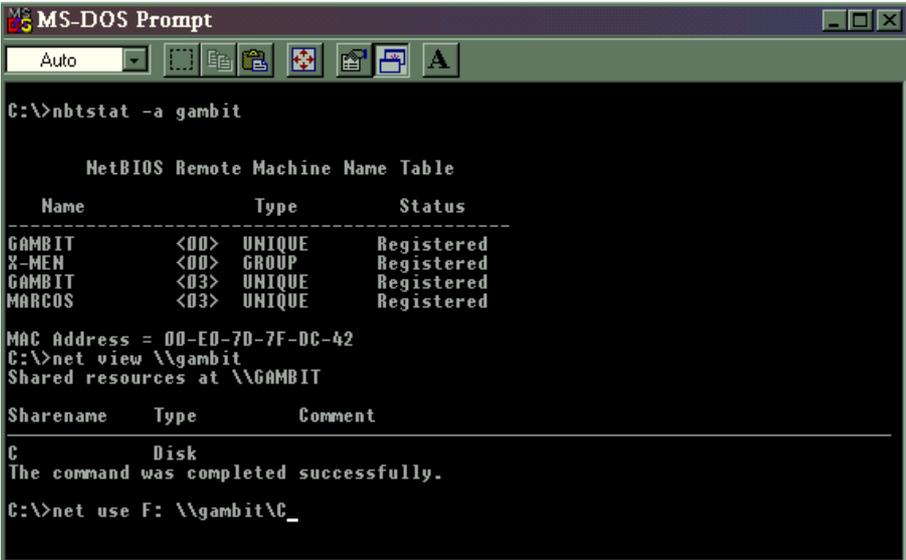
para Unix e Linux existem outros muito melhores. No site www.securityfocus.com existem códigos fontes ótimos para essa tarefa.

Scanneando o netbios

Netbios é uma espécie de protocolo que facilita a comunicação de uma pequena rede, porém não é roteável. Isso significa que: você pode conseguir invadir o computador e mapear drives de todas as pessoas que estão conectadas no mesmo provedor que você, pois estão na mesma subnet. Agora, se você estiver em um provedor e tentar alguma invasão em outro, ela não será possível com o SMB, apenas com o Netbios por TCP/IP (o que acaba dando quase na mesma, coloquei as diferenças para uma questão didática). Alguns cuidados devem ser tomados. Que hacker iniciante nunca ouviu falar de "invasão por ip", um texto que roda na internet há anos?. Pois é, ele corresponde à invasão por netbios. Para que você esteja protegido quanto a ataques, tome algumas providências:

- Se você não pertencer a nenhuma rede ou não precisar de compartilhar arquivos pela Internet, desabilite as opções "Compartilhar arquivos e impressoras" no assistente de rede do painel de controle do Windows. Assim você não será detectado por netbios.
- Caso você precise do protocolo, ao menos quando for compartilhar algum disco, coloque uma senha. Assim dificulta o acesso não-autorizado.
- Corrija os bugs do seu sistema. Especialmente se utiliza o Samba para compartilhar uma conexão netbios entre o Linux e o Windows. O Windows 98, ME, NT e 2000 também possuem alguns erros graves. Alguns deles possibilita que você possa mapear algum recurso da rede sabendo apenas o primeiro caractere da senha do netbios.
- Utilize algum bom scanner para netbios. Um excelente é o **NAT** (Netbios Auditing Tool). Ele utiliza um dicionário de senhas para tentar conseguir acesso ao sistema, e ainda checa se o mesmo possui falhas que possibilitem a conexão anônima. Para os que têm preguiça de usar programas em linhas de comando, sugiro o **Legion,** o **Shadow Scan** e o **projeto r3x**. Uma outra maneira rápida de checar se o netbios está ativo é usando o comando **nbtstat** do Windows. Geralmente a sintaxe é: **nbtstat –a <endereço ip>**. Existe um modo mais fácil de se tentar invadir um computador que esteja com o netbios ativo. É só ir em iniciar / executar e digitar **\\número do ip.** Mas vamos fazer do modo convencional:

1º passo: utilizar o nbtstat.

2º passo: encontrado um computador ativo (é sempre o que possui os números 00 e 03, além de ser UNIQUE no Type), vamos explorar os seus recursos.

3º passo: Encontrado algum recurso disponível (no caso do exemplo, o disco C) , vamos mapeá-lo (mapear significa adicionar o recurso como se fosse do seu próprio computador, como é o caso dos discos e impressoras em rede). Para mapear, utilizamos o comando:

net use F: \\gambit\C

Pronto. Mapeamos o disco C da máquina encontrada para o nosso disco F. É só ir ao Windows Explorer para acessar o disco ou simplesmente acessá-lo pelo DOS (o que é muito mais rápido). Para desconectar a unidade mapeada, usaremos o seguinte comando:

net use F: /DELETE

Para uma explicação melhor sobre a sintaxe do comando NET ou para conhecer outros recursos do Windows, cheque a seção de sistemas operacionais.

PS: Se o seu computador não tiver os comandos net (net use, net view) , tente instalar no painel de controle (em rede) o protocolo netbeui e o cliente para redes microsoft. Também verifique na sua conexão dial-up se o netbios está ativo.

Checando as vulnerabilidades em servidores HTTP e FTP

Tranqüilamente o mais perigoso de todos. Os scanners de servidores HTTP e FTP, chamados de scanners de vulnerabilidade, podem encontrar erros em sistemas em segundos e ainda indicar como explorar esses erros. Essa é a principal ferramenta do "Script Kiddie", típico garoto que quer ser hacker, consegue um software destes e sai fazendo varreduras em diversos sistemas. Mesmo que você não tenha inimigos, pode ser alvo de algum desses indivíduos algum dia, pois ele se diverte em tirar páginas do ar, colocar mensagens bobas e rir das pessoas que o acham um mestre. Não têm interesses de espionagem, é apenas uma criança. Chegamos em um problema: essas ferramentas não deviam ter a sua distribuição controlada? Se são tão perigosas, algumas até facilmente encontradas na Internet, deviam possuir algum tipo de restrição. Todos têm direito à informação, se souberem usá-la da maneira certa.

Alguns scanners são tão poderosos que possuem funções de scanneamento de portas, hosts e vulnerabilidades em um só host. Ou seja: descobre os hosts ativos, analisa as portas e analisa as vulnerabilidades encontradas nas portas. E meu amigo, se não tiver uma boa política de segurança, tudo desaba.

Bons scanners de vulnerabilidades para Windows: Security Shadow Scan, Retina, TWWWScan, Simpsons CGI Scanner, Stealth Scan, entre outros. Para Unix, temos o Nmap, o Nessus, o ISS e uma infinidade de programas. Não importa qual sistema seja rodado, geralmente esses programas podem scannear servidores em todo tipo de sistema. Do Windows ao Macintosh. Retomando o exemplo do provedor fictício **www.phela.com.br**, vamos realizar uma análise. Passamos um scanner qualquer e veremos os resultados.

Win NT 4.0 - Internet Information Server 4.0

::DATA

IIS Unicode

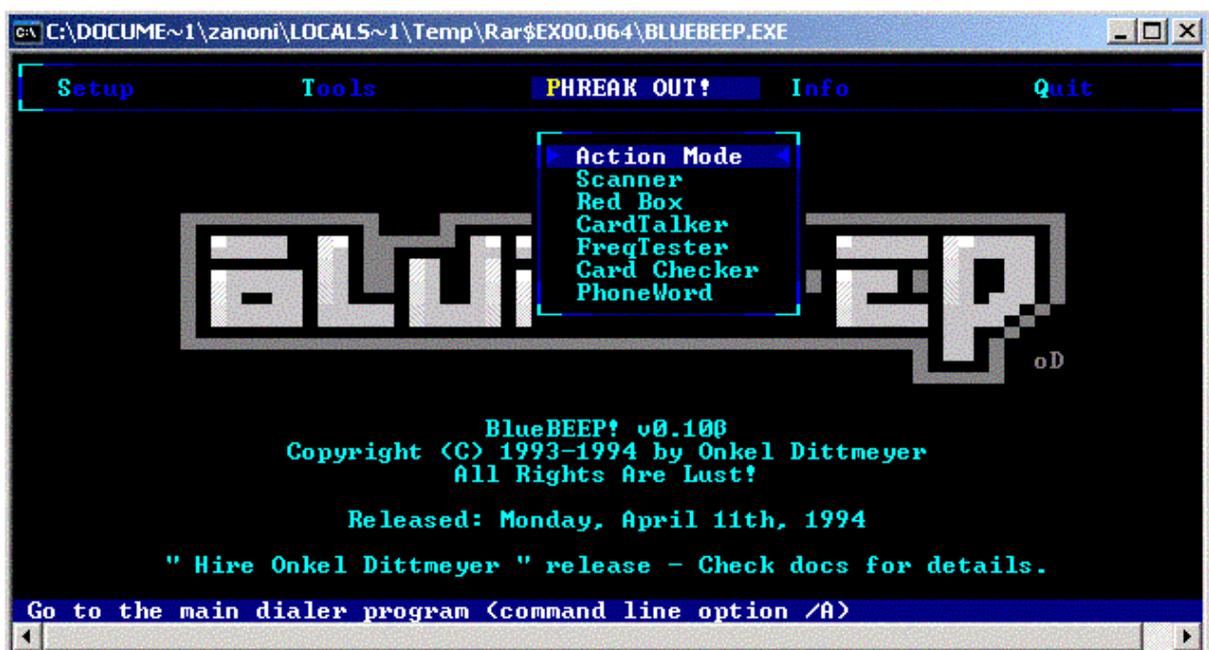
Buffer overflow

Descobrimos muita coisa. O sistema operacional usado, o servidor http e três erros. Se fosse o programa real fazendo a análise, ele daria um link ou exemplos de como explorar os erros para conseguir acesso ao servidor. E para colocar um pouco mais de medo nos administradores ,esses softwares têm uma opção de auto-upgrade, ou seja, se atualizam semanalmente com novas falhas descobertas.

Analisando partes físicas

O firewall e o roteador, por também conter falhas, são muito analisados pelos scanners. Alguns deles (firewalls) são tão sofisticados que enviam vários tipos de pacotes de informação somente para "deduzir" quais deles o firewall barra e quais não, assim descobrindo erros na sua implementação e para onde redirecionam os dados. O **Shadow Scan** por exemplo, consegue descobrir o endereço real de um servidor através da grande maioria dos firewalls. Portanto não adianta apenas instalar a sua barreira. Precisa atualizá-la sempre. Para saber mais sobre o assunto e conhecer alguns problemas exclusivos que elas sofrem , consulte a seção Firewall.

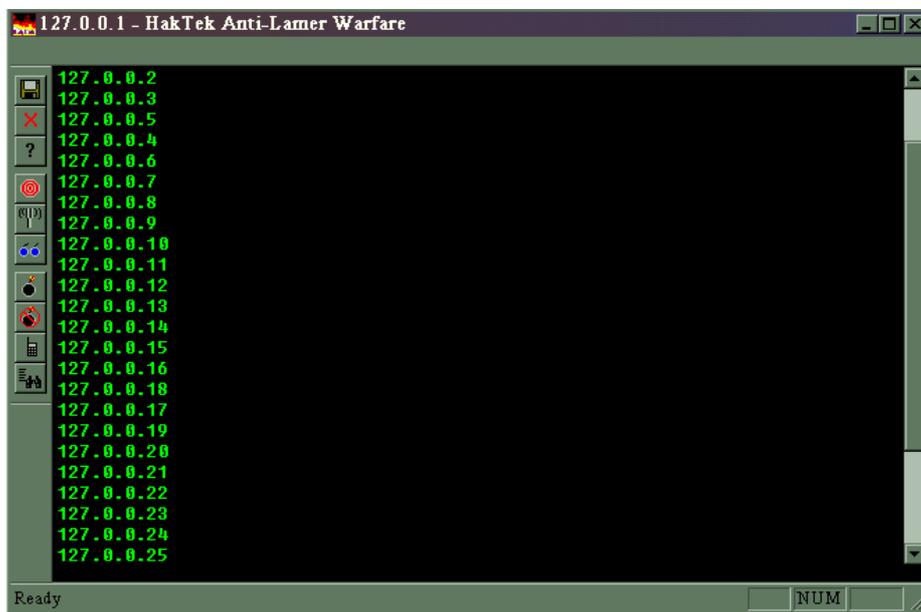
Wardialers

Os wardialers ou discadores de guerra, são programas que checam uma lista de telefones procurando por telefones conectáveis. Podem ser bem úteis. Por exemplo, supondo que o telefone comercial de uma empresa seja **829-1122**. Mande algum programa (como Toneloc) tentar se conectar a telefones do número **829-1100** a **829-1300**. Bom, pode ficar um pouco caro os impulsos mas a chance de você conseguir algum número de modem externo é grande. E geralmente usando sistemas com senhas ridículas (ou até sem senhas).

O Wardialer e gerador de tons Bluebeep.

Instalando proteções

Para se proteger, você precisa seguir a seguinte política: esteja sempre passando scanners no seu sistema, atualizando seu firewall e instalando proteções extras (como detectores para scanners de porta. Quando alguém tentar varrer o seu sistema checando os serviços ativos, ele impede e lhe fornece o ip da pessoa). Mas e se você descobrir alguma falha? Na informação fornecida pelo scanner de vulnerabilidade está aonde você pode conseguir o **patch** (atualização) para essa falha. Então visite o site do fabricante (no caso do nosso exemplo do provedor Phela, seria a Microsoft), pegue o patch e leia com atenção para saber como aplicá-lo no seu sistema. Se arrumar um tempinho para fazer tudo isso, garanto que pode lhe render algumas boas noites de sono.

Passo-a-passo: Scanneando

Scanneando hosts conhecidos de uma rede

Para esse exercício pode ser usado qualquer scanner. Usaremos o haktek.

1. Abra o programa
2. Clique no botãozinho que parece um controle remoto e coloque em range os ips que deseja procurar. Por exemplo: 200.187.138.1 a 200.187.138.250 (endereço fictício).
3. Mande ver.

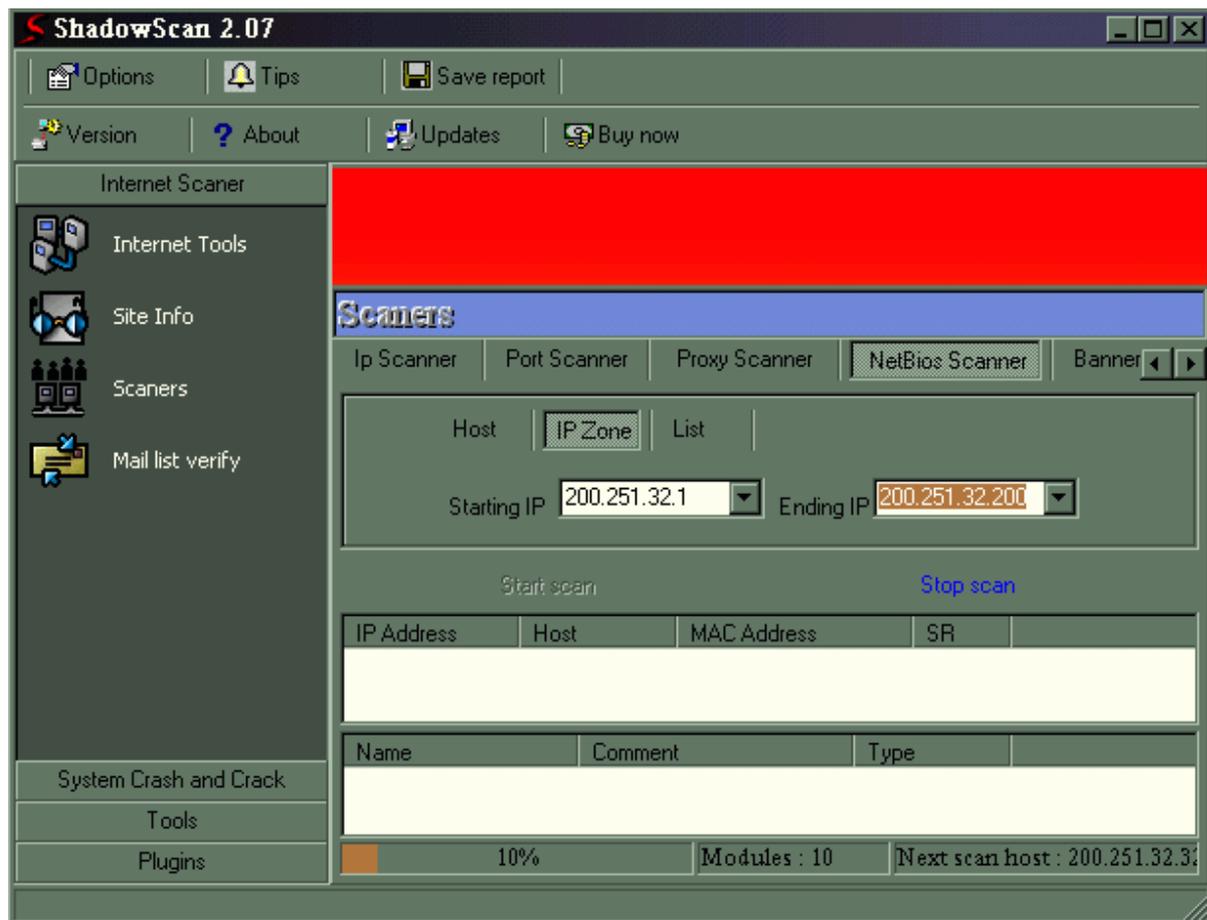
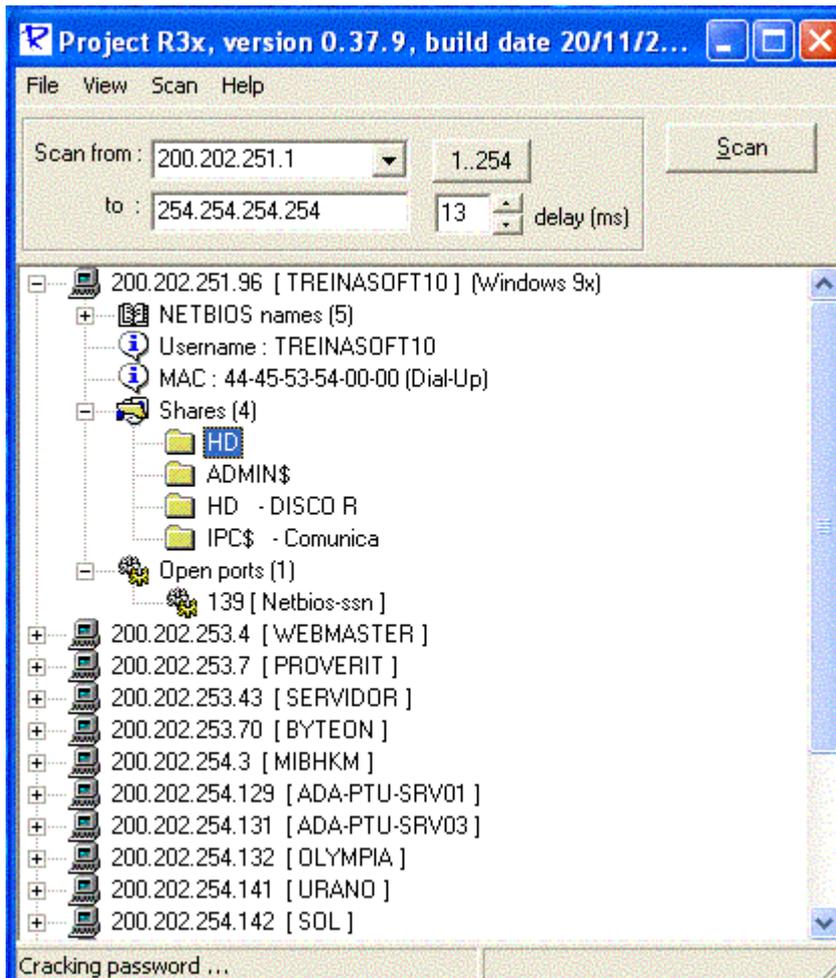
O programa mostrará todos os hosts encontrados (que estão ativos) e mostrar seus respectivos nomes (se tiverem).

Scanneando o NetBIOS

Para realizarmos uma checagens de máquinas com NetBIOS ativas, utilizaremos primeiramente o programa **Shadow Scan**.

Abra o programa.

1. Clique em Internet Scaner de depois em Scaners.
2. Selecione NetBios Scanner.
3. Clique em IP Zone e coloque a subnet que você irá procurar (de qual a qual endereço ip). Não se esqueça que como o NetBIOS não é roteável você só pode fazê-lo no seu provedor ou rede local.

O ShadowScan é um dos melhores programas de segurança para Windows. Possui praticamente de tudo.

Se preferir , use o projeto R3X. Ele é mais rápido que o Shadow Scan e às vezes até mais eficiente, além de explorar um erro que descobre qualquer senha de Netbios do Windows 95, 98 e 98 SE.

Scanneando à procura de falhas

Nesse teste, utilizaremos algum dos scanners de vulnerabilidade para descobrir falhas em um host. Na minha opinião, o Shadow Security Scanner é o melhor para Windows (ele é baseado no programa Retina do grupo EEYE) e o Nessus o melhor para Unix. Utilizaremos o TWWWSCAN como exemplo pois ele é bem simples.

1. Abra o prompt do ms-dos.
2. Execute o programa.
3. Após o programa mostrar essa tela, execute-o novamente com o seguinte comando: **twwwscan <endereço ip ou nome do host> 80 –v –t3 –pa –ids**

Pedimos ao scanner para utilizar a porta 80 (padrão), -v (mostrar o status), -t3 (utilizar dois tipos de métodos de teste), -pa (tentar erros de unix e de windows) e –ids (tática para conseguir um resultado mais eficiente). O programa irá rodar, testar diversas combinações e lhe fornecer os erros encontrados.

Outros bom programas para serem testados:

Retina *(**www.eeye.com**)*

Typhon *(visto no capítulo sobre falhas, pode ser pego em **www.security-focus.com**)*

Stealth (visto no capítulo sobre falhas, pode ser pego em ***www.nstalker.com****)*

E muitos outros. O negócio é fuçar para descobrir as novidades. E isso é o que não falta. Visite sempre páginas como www.blackcode.com e www.securityfocus.com para obter novidades.

10

Criptografia

Introdução

Criptografia é a arte da escrita oculta usada desde a antiguidade por exemplo: pelos egípcios na sua antiga escrita. Ela é muito importante hoje em dia na internet. Mandar um e-mail confidencial da maneira convencional é muito inseguro ele pode ser interceptado no meio da transmissão ou posteriormente, por isto a necessidade do uso de programas eficientes, como o PGP. Esses programas possibilitam uma espécie de "código especial" entre você e o receptor da mensagem, fazendo com que mesmo que alguém consiga obte-la no meio do caminho, ela será impossível de se ler.

Chaves públicas e privadas

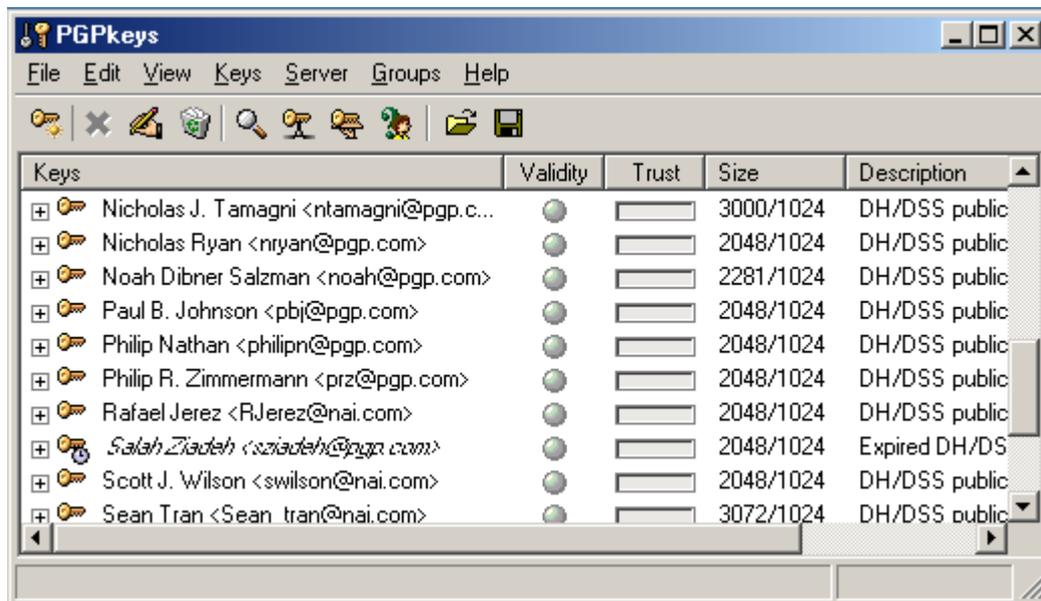
Na década de 1970 o patrão na criptografia era a criptografia simétrica onde tínhamos uma única chave (senha) para encriptar e desencriptar, tanto para o emissor quanto para o destinatário. O grande problema desse método era como transmitir com segurança esta senha.

No final da década de 70 foi desenvolvido o método da criptografia assimétrica e a tecnologia das chaves pública e privada. Você encriptava com a chave pública do destinatário e somente ele poderia desencriptar utilizando a sua chave privada , e também haveria como saber com certeza absoluta se a pessoa que mandou a mensagem era realmente quem dizia ser.

PGP

Nesse cenário foi desenvolvido o famoso programa PGP por Philip R. Zimmermann. Segundo as autoridades americanas ferindo as patentes do algoritmo RSA, ele foi processado e os voluntários da internet o ajudaram a pagar os advogados. Hoje as leis americanas já estão mais brandas e o PGP já é usado internacionalmente. Por fim a Network Associates(desenvolvedora do Mcafee Vírus Scan), comprou os direitos do PGP e hoje Zimmermann é seu empregado.

Até hoje, após várias versões desse programa ninguém nunca desencriptou uma única mensagem de 16bits do PGP e hoje ele trabalha com mais de 2000bits. Sempre gera uma nova criptografia a cada seção. Estima-se que dezenas de computadores Pentium levariam muito tempo para desencriptar uma simples mensagem de 16bits. Não é exagero. É a tecnologia. Pegue o PGP no endereço w**ww.superdownloads.com.br.** Com certeza é um ótimo software e vale a pena aprender a usá-lo. Mas lembre-se , apesar de difícil a

criptografia não é impossível de ser quebrada. A prova disso é o grupo de internautas que conseguiu quebrar o código criptografado de um celular de última geração.

O programa PGP é largamente utilizado atualmente.

Saídas alternativas

Se o que você quer é apenas esconder alguns arquivos na sua máquina para que ninguém os utilize ou encontre, há algumas saídas interessantes. Crie diretórios usando caracteres ALT (capítulo sobre 9, sobre DOS). O Windows não consegue acessar esses diretórios. Esconda arquivos comprimindo-os com GZIP ou TAR e renomeando-os (mude a extensão para DLL e coloque no diretório SYSTEM do Windows, quero ver quem vai encontrar). O que manda, mein freunds, é a imaginação. Tanto que a maioria dos hackers têm mais imaginação do que conhecimentos. Ou você acha que existe algum ser humano na face da Terra que saiba: **Pascal, Basic, C, Fortran, Algol, Java, Assembler, PHP, Flash, BeOS, Unix, Dec-10, Hardware, Novell, SQL, Windows NT, Macintosh e VAX/VMS**? Bom, se tiver alguém com certeza você encontrará o nome no Guiness.

11

Crackeando

Conceito de “crackear”

Crackear no mundo da segurança significa se utilizar de alguma técnica ou ferramenta para se descobrir algum dado criptografado ou uma senha. Atualmente é muito comum o “cracking”. Conseguiram crackear o sistema de criptografia de um celular novo, um garoto de 16 anos conseguiu quebrar a criptografia do sistema de DVD, resultando no programa DeCSS e no DivX (formato comprimido de filmes, como se fosse o mp3 da música). Sistemas simples de criptografia também são fáceis de serem quebrados. O Windows 3.11 utilizava o Trumpet Winsock para a conexão com a Internet. Após cerca de duas horas brincando com ele, descobri como sua criptografia funcionava. Os antigos joguinhos de DOS que precisavam de senhas, tal como Prince of Pérsia e Stunts são também facilmente crackeados.

E por aí vai. O maior problema relacionado à segurança é com o descobrimento de senhas. É extremamente fácil de se descobri-las devido ao constante aumento da velocidade dos computadores e dos cada vez mais frágeis sistemas operacionais. Um simples trojan ou um sniffer podem conseguir quebrar uma senha facilmente. Existem também alguns outros recursos utilizados por crackers, como utilização de wordlists e bruteforce.

Wordlists

São listas de palavras criadas especialmente para se descobrir senhas. Quando você têm em mãos um arquivo de senha do UNIX com o sistema de criptografia DES, por exemplo. A criptografia é inquebrável, mas você pode utilizar programas como o famoso **Cracker Jack** ou mesmo o **Shadow Scan**. Eles pegam um arquivo criado por você com listas de palavras comuns (geralmente utilizadas como senhas, tal como alien3, tricolor, secreta, 101010 e outras) o criptografa utilizando o mesmo sistema das senhas de Unix (DES) e compara os arquivos. Se o programa encontrar algum usuário em que a criptografia tenha ficado exatamente igual, o nome lhe é informado. As palavras são colocadas verticalmente, uma em cada linha. Mais ou menos assim:

alien3

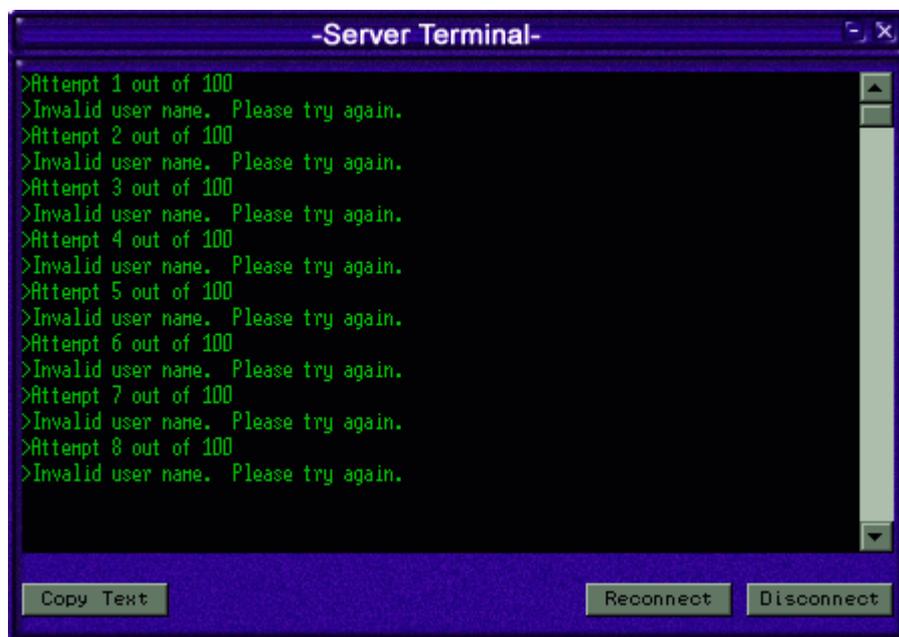
tricolor

secreta

101010

12345

O processo de bruteforce

O método da força bruta é muito demorado. Pode levar horas, e as vezes dias. Mas continua sendo de longe o mais eficaz. Utiliza-se um programa que tenta conectar-se a um sistema utilizando todas as combinações possíveis de letras e números. Para um cracker que possui uma conexão de 56 kbps e utiliza um Pentium III 800, é improvável que consiga descobrir a senha. Para se ter alguma chance deve-se utilizar uma conexão dedicada (à cabo, via rádio e outras) e vários computadores. Tendo 20 computadores rápidos trabalhando cada um em um setor (um tentando descobrir senhas começadas por a, outro por b, outro por c, etc...) o tempo para se conseguir o prêmio diminuirá consideravelmente. Existem alguns casos em que a força bruta é mais rápido, como quando se tenta quebrar um arquivo de senhas localmente. Pode ser um passwd do Unix ou um mais fácil de se quebrar ainda, o PWL do Windows. O programa **CAIN ,ShadowScan, Brutus e NAT (Netbios Auditing Tool)** são bons programa para realizar o processo de bruteforce. Para encontrá-los já sabe: Lycos, Google, Yahoo e Altavista na cabeça.

Realização de um bruteforce em algum sistema vulnerável

Senhas padrões

Senhas padrões são senhas que já vêm configuradas com o sistema ou algum utilitário de atualização as configura. Existem não só nos sistemas operacionais mas também em dispositivos de hardware como roteadores. Asseguro que a lista a seguir é a maior que você já viu. Use-a para checar se o seu sistema está vulnerável ou crie uma wordlist com as senhas padrões mais usadas de todos os sistemas. De qualquer maneira, tenho certeza que esses dados lhe serão muito interessantes.

Fabricante	Produto	Revisão	Protocolo	Usuário	Senha	Nível de acesso

3COM	CellPlex	7000	Telnet	tech	tech	
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet	
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech	
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)	
3COM	LANplex	2500	Telnet	debug	synnet	
3COM	LANplex	2500	Telnet	tech	tech	
3COM	LinkSwitch	2000/2700	Telnet	tech	tech	
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD	Admin
3COM	NetBuilder		SNMP	n/a	ANYCOM	
3COM	SuperStack II Switch	2200	Telnet	debug	synnet	
3COM	SuperStack II Switch	2700	Telnet	tech	tech	
3COM	SuperStack II Switch	1100/3300	Telnet	monitor	monitor	Monitor
3COM	SuperStack II Switch	1100/3300	Telnet	manager	manager	Manager
3COM	SuperStack II Switch	1100/3300	Telnet	admin	(none)	Admin
3COM	SuperStack II Switch	1100/3300	Telnet	security	security	Admin
3COM			Telnet	adm	(none)	
3COM			Telnet	admin	synnet	
3COM			Telnet	manager	manager	
3COM			Telnet	monitor	monitor	
3COM			Telnet	read	synnet	
3COM			Telnet	security	security	
3COM			Telnet	write	synnet	
Accelerated Networks	DSL CPE and DSLAM		Telnet	sysadm	anicust	
ADC Kentrox	Pacesetter Router		Telnet	n/a	secret	
Adtran	MX2800		Telnet	n/a	adtran	
Advanced Integration	PC BIOS		Console	n/a	Advance	Admin
Alteon	ACEswitch	180e	HTTP	admin	admin	Admin
Alteon	ACEswitch	180e	Telnet	admin	(none)	
AMI	PC BIOS		Console	n/a	AM	Admin
AMI	PC BIOS		Console	n/a	AMI	Admin
AMI	PC BIOS		Console	n/a	A.M.I	Admin
AMI	PC BIOS		Console	n/a	AMI_SW	Admin
AMI	PC BIOS		Console	n/a	AMI?SW	Admin
AMI	PC BIOS		Console	n/a	aammii	Admin
AMI	PC BIOS		Console	n/a	AMI!SW	Admin
AMI	PC BIOS		Console	n/a	AMI.KEY	Admin
AMI	PC BIOS		Console	n/a	AMI.KEZ	Admin
AMI	PC BIOS		Console	n/a	AMI~	Admin
AMI	PC BIOS		Console	n/a	AMIAMI	Admin
AMI	PC BIOS		Console	n/a	AMIDECOD	Admin
AMI	PC BIOS		Console	n/a	AMIPSWD	Admin
AMI	PC BIOS		Console	n/a	amipswd	Admin
AMI	PC BIOS		Console	n/a	AMISETUP	Admin
AMI	PC BIOS		Console	n/a	BIOSPASS	Admin
AMI	PC BIOS		Console	n/a	CMOSPWD	Admin
AMI	PC BIOS		Console	n/a	HEWITT RAND	Admin
Amptron	PC BIOS		Console	n/a	Polrty	Admin
Apache Project	Apache "jj" script		HTTP	n/a	SDGROCKS	User
APC	MasterSwitch	AP9210		apc	apc	Admin
APC	SNMP Adapter	2.x		apc	apc	
APC	Call-UPS	AP9608	Console	n/a	serial number of the Call-UPS	Admin
APC	Share-UPS	AP9207	Console	n/a	serial number of the Share-UPS	Admin
APC	Web/SNMP Management Card	AP9606	Multi	apc	apc	Admin

APC	Powerchute Plus	4.x for Netware 3.x/4.x	Console	POWERCHUT E	APC	Admin
Ascend	Router		Telnet	n/a	ascend	Admin
AST	PC BIOS		Console	n/a	SnuFG5	Admin
Attachmate	Attachmate Gateway		Console	n/a	PASSWORD	Admin
AT&T	3B2 Firmware		Console	n/a	mcp	Admin
Audioactive	MPEG Realtime Encoders		Telnet	n/a	telos	Admin
Autodesk	Autocad		Multi	autocad	autocad	User
AWARD	PC BIOS		Console	n/a	Award	Admin
AWARD	PC BIOS		Console	n/a	AWARD_SW	Admin
AWARD	PC BIOS		Console	n/a	SW_AWARD	Admin
AWARD	PC BIOS		Console	n/a	lkwpeter	Admin
AWARD	PC BIOS		Console	n/a	LKWPETER	Admin
AWARD	PC BIOS		Console	n/a	?award	Admin
AWARD	PC BIOS		Console	n/a	256256	Admin
AWARD	PC BIOS		Console	n/a	admin	Admin
AWARD	PC BIOS		Console	n/a	alfarome	Admin
AWARD	PC BIOS		Console	n/a	aLLy	Admin
AWARD	PC BIOS		Console	n/a	aPAf	Admin
AWARD	PC BIOS		Console	n/a	award	Admin
AWARD	PC BIOS		Console	n/a	AWARD SW	Admin
AWARD	PC BIOS		Console	n/a	awkward	Admin
AWARD	PC BIOS		Console	n/a	BIOS	Admin
AWARD	PC BIOS		Console	n/a	biosstar	Admin
AWARD	PC BIOS		Console	n/a	biostar	Admin
AWARD	PC BIOS		Console	n/a	CONCAT	Admin
AWARD	PC BIOS		Console	n/a	condo	Admin
AWARD	PC BIOS		Console	n/a	CONDO	Admin
AWARD	PC BIOS		Console	n/a	CONDO,	Admin
AWARD	PC BIOS		Console	n/a	HELGA-S	Admin
AWARD	PC BIOS		Console	n/a	HEWITT RAND	Admin
AWARD	PC BIOS		Console	n/a	HLT	Admin
AWARD	PC BIOS		Console	n/a	j322	Admin
AWARD	PC BIOS		Console	n/a	j64	Admin
AWARD	PC BIOS		Console	n/a	lkw peter	Admin
AWARD	PC BIOS		Console	n/a	lkwpeter	Admin
AWARD	PC BIOS		Console	n/a	PASSWORD	Admin
AWARD	PC BIOS		Console	n/a	SER	Admin
AWARD	PC BIOS		Console	n/a	setup	Admin
AWARD	PC BIOS		Console	n/a	SKY_FOX	Admin
AWARD	PC BIOS		Console	n/a	SWITCHES_SW	Admin
AWARD	PC BIOS		Console	n/a	Sxyz	Admin
AWARD	PC BIOS		Console	n/a	SZYX	Admin
AWARD	PC BIOS		Console	n/a	t0ch20x	Admin
AWARD	PC BIOS		Console	n/a	t0ch88	Admin
AWARD	PC BIOS		Console	n/a	TTPTHA	Admin
AWARD	PC BIOS		Console	n/a	TzqF	Admin
AWARD	PC BIOS		Console	n/a	wodj	Admin
AWARD	PC BIOS		Console	n/a	zbaaaca	Admin
Axis	NETCAM	200/240	Telnet	root	pass	Admin
Axis	Printserver	540/540+	Multi	root	pass	Admin
Bay Networks	Router		Telnet	Manager	(none)	Admin
Bay Networks	Router		Telnet	User	(none)	User
Bay Networks	SuperStack II		Telnet	security	security	Admin

Bay Networks	Switch	350T	Telnet	n/a	NetICs	Admin
Bintec	Bianka Routers		Multi	admin	bintec	Admin
Biostar	PC BIOS		Console	n/a	Biostar	Admin
Biostar	PC BIOS		Console	n/a	Q54arwms	Admin
Breezecom	Breezecom Adapters	4.4.x		n/a	Helpdesk	Admin
Breezecom	Breezecom Adapters	4.x		n/a	Super	Admin
Breezecom	Breezecom Adapters	3.x		n/a	Master	Admin
Breezecom	Breezecom Adapters	2.x		n/a	laflaf	Admin
Cabletron	Netgear modem/router and SSR			netman	(none)	Admin
Cabletron	routers & switches			(none)	(none)	
Cayman	Cayman DSL			n/a	(none)	Admin
CGI World	Poll It	v2.0	HTTP	n/a	protection	User/Admin over package
Cisco	CiscoWorks 2000			admin	cisco	Admin
Cisco	CiscoWorks 2000			guest	(none)	User
Cisco	ConfigMaker			cmaker	cmaker	Admin
Cisco	IOS		Multi	cisco	cisco	
Cisco	IOS		Multi	enable	cisco	
Cisco	IOS	2600 series	Multi	n/a	c	
Cisco	IOS		Multi	n/a	cc	
Cisco	IOS		Multi	n/a	cisco	
Cisco	IOS		Multi	n/a	Cisco router	
Cisco	IOS		SNMP	public ReadOnly access	secret	Read
Cisco	IOS		SNMP	private ReadWrite access	secret	Read/Write
Cisco	IOS		Multi	ripeop	(no pw)	
Cisco	PIX		Telnet	n/a	cisco	UID = pix
Cisco-Arrowpoint	Arrowpoint			admin	system	Admin
Compaq	Insight Manager			administrator	administrator	Admin
Compaq	Insight Manager			anonymous	(none)	User
Compaq	Insight Manager			operator	operator	
Compaq	Insight Manager			user	public	User
Compaq	PC BIOS		Console	n/a	Compaq	Admin
Compualynx	Cproxy Server	All Versions	Multi	administrator	asecret	Admin
Compualynx	Cmail Server	All Versions	Multi	administrator	asecret	Admin
Compualynx	SCM	All Versions	Multi	administrator	asecret	Admin
Concord	PC BIOS			n/a	last	Admin
Crystalview	OutsideView 32				Crystal	Admin
CTX International	PC BIOS		Console	n/a	CTX_123	Admin
CyberMax	PC BIOS		Console	n/a	Congress	Admin
Daewoo	PC BIOS		Console	n/a	Daewuu	Admin
Dallas Semiconductors	TINI embedded JAVA Module	<= 1.0	Telnet	root	tini	Admin
Data General	AOS/VS		Multi	operator	operator	Admin
Data General	AOS/VS		Multi	op	op	Admin
Data General	AOS/VS		Multi	op	operator	Admin
Datacom	BSASX/101			n/a	letmein	Admin
Datacom	NSBrowse		Multi	sysadm	sysadm	Admin
Daytek	PC BIOS		Console	n/a	Daytec	Admin
Debian	Linux LILO Default	2.2	Console	n/a	tatercounter2000	Admin
Dell	PC BIOS		Console	n/a	Dell	Admin
Develcon	Orbitor Default Console			n/a	BRIDGE	Admin
Develcon	Orbitor Default Console			n/a	password	Admin
Dictaphone	ProLog			NETOP	(none)	
Dictaphone	ProLog			NETWORK	NETWORK	

Dictaphone	ProLog		PBX	PBX	
Digicorp	Viper	Telnet	n/a	BRIDGE	Admin
Digicorp	Viper	Telnet	n/a	password	Admin
Digital Equipment	DEC-10	Multi	1	syslib	Admin
Digital Equipment	DEC-10	Multi	1	operator	Admin
Digital Equipment	DEC-10	Multi	1	manager	Admin
Digital Equipment	DEC-10	Multi	2	maintain	Admin
Digital Equipment	DEC-10	Multi	2	syslib	Admin
Digital Equipment	DEC-10	Multi	2	manager	Admin
Digital Equipment	DEC-10	Multi	2	operator	Admin
Digital Equipment	DEC-10	Multi	30	games	User
Digital Equipment	DEC-10	Multi	5	games	User
Digital Equipment	DEC-10	Multi	7	maintain	User
Digital Equipment	DecServer	Multi	n/a	ACCESS	Admin
Digital Equipment	DecServer	Multi	n/a	SYSTEM	Admin
Digital Equipment	IRIS	Multi	accounting	accounting	Admin
Digital Equipment	IRIS	Multi	boss	boss	Admin
Digital Equipment	IRIS	Multi	demo	demo	User
Digital Equipment	IRIS	Multi	manager	manager	Admin
Digital Equipment	IRIS	Multi	PDP11	PDP11	User
Digital Equipment	IRIS	Multi	PDP8	PDP8	User
Digital Equipment	IRIS	Multi	software	software	User
Digital Equipment	PC BIOS	Console	n/a	komprie	Admin
Digital Equipment	RSX	Multi	1,1	SYSTEM	Admin
Digital Equipment	RSX	Multi	BATCH	BATCH	User
Digital Equipment	RSX	Multi	SYSTEM	MANAGER	Admin
Digital Equipment	RSX	Multi	SYSTEM	SYSTEM	Admin
Digital Equipment	RSX	Multi	USER	USER	User
Digital Equipment	Terminal Server	Port 7000	n/a	access	User
Digital Equipment	Terminal Server	Port 7000	n/a	system	Admin
Digital Equipment	VMS	Multi	ALLIN1	ALLIN1	
Digital Equipment	VMS	Multi	ALLIN1MAIL	ALLIN1MAIL	
Digital Equipment	VMS	Multi	ALLINONE	ALLINONE	
Digital Equipment	VMS	Multi	BACKUP	BACKUP	
Digital Equipment	VMS	Multi	DCL	DCL	
Digital Equipment	VMS	Multi	DECMAIL	DECMAIL	
Digital Equipment	VMS	Multi	DECNET	DECNET	
Digital Equipment	VMS	Multi	DECNET	NONPRIV	
Digital Equipment	VMS	Multi	DECNET	DECNET	
Digital Equipment	VMS	Multi	DEFAULT	USER	
Digital Equipment	VMS	Multi	DEFAULT	DEFAULT	
Digital Equipment	VMS	Multi	DEMO	DEMO	
Digital Equipment	VMS	Multi	FIELD	FIELD	
Digital Equipment	VMS	Multi	FIELD	SERVICE	
Digital Equipment	VMS	Multi	FIELD	TEST	
Digital Equipment	VMS	Multi	FIELD	DIGITAL	
Digital Equipment	VMS	Multi	GUEST	GUEST	
Digital Equipment	VMS	Multi	HELP	HELP	
Digital Equipment	VMS	Multi	HELPDESK	HELPDESK	
Digital Equipment	VMS	Multi	HOST	HOST	
Digital Equipment	VMS	Multi	HOST	HOST	
Digital Equipment	VMS	Multi	INFO	INFO	
Digital Equipment	VMS	Multi	INGRES	INGRES	
Digital Equipment	VMS	Multi	LINK	LINK	

Digital Equipment	VMS		Multi	MAILER	MAILER	
Digital Equipment	VMS		Multi	MBMANAGER	MBMANAGER	
Digital Equipment	VMS		Multi	MBWATCH	MBWATCH	
Digital Equipment	VMS		Multi	NETCON	NETCON	
Digital Equipment	VMS		Multi	NETMGR	NETMGR	
Digital Equipment	VMS		Multi	NETNONPRIV	NETNONPRIV	
Digital Equipment	VMS		Multi	NETPRIV	NETPRIV	
Digital Equipment	VMS		Multi	NETSERVER	NETSERVER	
Digital Equipment	VMS		Multi	NETSERVER	NETSERVER	
Digital Equipment	VMS		Multi	NETWORK	NETWORK	
Digital Equipment	VMS		Multi	NEWINGRES	NEWINGRES	
Digital Equipment	VMS		Multi	NEWS	NEWS	
Digital Equipment	VMS		Multi	OPERVAX	OPERVAX	
Digital Equipment	VMS		Multi	POSTMASTER	POSTMASTER	
Digital Equipment	VMS		Multi	PRIV	PRIV	
Digital Equipment	VMS		Multi	REPORT	REPORT	
Digital Equipment	VMS		Multi	RJE	RJE	
Digital Equipment	VMS		Multi	STUDENT	STUDENT	
Digital Equipment	VMS		Multi	SYS	SYS	
Digital Equipment	VMS		Multi	SYSMAINT	SYSMAINT	
Digital Equipment	VMS		Multi	SYSMAINT	SERVICE	
Digital Equipment	VMS		Multi	SYSMAINT	DIGITAL	
Digital Equipment	VMS		Multi	SYSTEM	SYSTEM	
Digital Equipment	VMS		Multi	SYSTEM	MANAGER	
Digital Equipment	VMS		Multi	SYSTEM	OPERATOR	
Digital Equipment	VMS		Multi	SYSTEM	SYSLIB	
Digital Equipment	VMS		Multi	SYSTEST	UETP	
Digital Equipment	VMS		Multi	SYSTEST_CLIG	SYSTEST_CLIG	
Digital Equipment	VMS		Multi	SYSTEST_CLIG	SYSTEST	
Digital Equipment	VMS		Multi	TELEDEMO	TELEDEMO	
Digital Equipment	VMS		Multi	TEST	TEST	
Digital Equipment	VMS		Multi	UETP	UETP	
Digital Equipment	VMS		Multi	USER	PASSWORD	
Digital Equipment	VMS		Multi	USERP	USERP	
Digital Equipment	VMS		Multi	VAX	VAX	
Digital Equipment	VMS		Multi	VMS	VMS	
D-Link	hubs/switches		Telnet	D-Link	D-Link	
Dynix Library Systems	Dynix		Multi	circ	<social sec #>	User
Dynix Library Systems	Dynix		Multi	LIBRARY	(none)	User
Dynix Library Systems	Dynix		Multi	SETUP	(none)	Admin
Efficient	Speedstream DSL		Telnet	n/a	admin	Admin
Elsa	LANCom Office ISDN Router	800/1000/1100	Telnet	n/a	cisco	Admin
Elsa	LANCom Office ISDN Router	800/1000/1100	Telnet	n/a	(none)	Admin
Enox	PC BIOS		Console	n/a	xo11nE	Admin
Epox	PC BIOS		Console	n/a	central	Admin
Ericsson	Ericsson Acc			netman	netman	
Flowpoint	DSL	2000	Telnet	admin	admin	Admin
Flowpoint	DSL		Telnet	n/a	password	Admin
Flowpoint	Flowpoint/2000 ADSL		Telnet	n/a	(none)	Admin
Freetech	PC BIOS		Console	n/a	Posterie	Admin
Galacticomm	Major BBS		Multi	Sysop	Sysop	Admin
GuardOne	Restrictor		Multi	n/a	guardone	Admin
GuardOne	BizGuard		Multi	n.a	guardone	Admin

glFtpD	glFtpD	all	Console	glftpd	glftpd	Admin
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	ADVMAIL	HPOFFICE,DATA	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	ADVMAIL	HP	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	SUPPORT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	MGR	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	SERVICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	MANAGER	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	HPP187,SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	LOTUS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	HPWORD,PUB	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	HPONLY	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	MANAGER.SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	MGR.SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	FIELD.SUPPORT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	OP.OPERATOR	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MAIL	MAIL	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MAIL	REMOTE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MAIL	TELESUP	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MAIL	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MAIL	MPE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	TCH	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	SECURITY	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	ITF3000	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	COGNOS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	TELESUP	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGE	VESOFT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGE	VESOFT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	CAROLIAN	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	VESOFT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	XLSERVER	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	SECURITY	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	TELESUP	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPDESK	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	CCC	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	CNAS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	WORD	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	COGNOS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	ROBELLE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPONLY	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPP187	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPP189	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPP196	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	INTX3	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	ITF3000	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	NETBASE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	REGO	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	RJE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	CONV	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	OPERATOR	SYS	

Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	OPERATOR	DISC	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	OPERATOR	SYSTEM	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	OPERATOR	SUPPORT	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	OPERATOR	COGNOS	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	PCUSER	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	RSBCMON	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	SPOOLMAN	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx	Multi	WP	HPOFFICE	
Hewlett-Packard	Vectra	Console	n/a	hewlpack	Admin
IBM	AIX	Multi	guest	(none)	User
IBM	AIX	Multi	guest	guest	User
IBM	Ascend OEM Routers	Telnet	n/a	ascend	Admin
IBM	OS/400	Multi	11111111	11111111	
IBM	OS/400	Multi	22222222	22222222	
IBM	OS/400	Multi	ibm	password	
IBM	OS/400	Multi	ibm	2222	
IBM	OS/400	Multi	ibm	service	
IBM	OS/400	Multi	qpgmr	qpgmr	
IBM	OS/400	Multi	qsecofr	qsecofr	
IBM	OS/400	Multi	qsecofr	11111111	
IBM	OS/400	Multi	qsecofr	22222222	
IBM	OS/400	Multi	qserv	qserv	
IBM	OS/400	Multi	qsrv	qsrv	
IBM	OS/400	Multi	qsrvbas	qsrvbas	
IBM	OS/400	Multi	qsvr	qsvr	
IBM	OS/400	Multi	qsvr	ibmcel	
IBM	OS/400	Multi	qsysopr	qsysopr	
IBM	OS/400	Multi	quser	quser	
IBM	OS/400	Multi	user	USERP	
IBM	OS/400	Multi	secofr	secofr	
IBM	OS/400	Multi	sedacm	secacm	
IBM	OS/400	Multi	sysopr	sysopr	
IBM	PC BIOS	Console	n/a	IBM	Admin
IBM	PC BIOS	Console	n/a	MBIU0	Admin
IBM	PC BIOS	Console	n/a	sertafu	Admin
IBM	POS CMOS	Console	ESSEX		
IBM	POS CMOS	Console	IPC		
IBM	VM/CMS	Multi	$ALOC$	(none)	
IBM	VM/CMS	Multi	ADMIN	(none)	
IBM	VM/CMS	Multi	AP2SVP	(none)	
IBM	VM/CMS	Multi	APL2PP	(none)	
IBM	VM/CMS	Multi	AUTOLOG1	(none)	
IBM	VM/CMS	Multi	BATCH	(none)	
IBM	VM/CMS	Multi	BATCH1	(none)	
IBM	VM/CMS	Multi	BATCH2	(none)	
IBM	VM/CMS	Multi	CCC	(none)	
IBM	VM/CMS	Multi	CMSBATCH	(none)	
IBM	VM/CMS	Multi	CMSUSER	(none)	
IBM	VM/CMS	Multi	CPNUC	(none)	
IBM	VM/CMS	Multi	CPRM	(none)	
IBM	VM/CMS	Multi	CSPUSER	(none)	
IBM	VM/CMS	Multi	CVIEW	(none)	
IBM	VM/CMS	Multi	DATAMOVE	(none)	
IBM	VM/CMS	Multi	DEMO1	(none)	

IBM	VM/CMS	Multi	DEMO2	(none)
IBM	VM/CMS	Multi	DEMO3	(none)
IBM	VM/CMS	Multi	DEMO4	(none)
IBM	VM/CMS	Multi	DIRECT	(none)
IBM	VM/CMS	Multi	DIRMAINT	(none)
IBM	VM/CMS	Multi	DISKCNT	(none)
IBM	VM/CMS	Multi	EREP	(none)
IBM	VM/CMS	Multi	FSFADMIN	(none)
IBM	VM/CMS	Multi	FSFTASK1	(none)
IBM	VM/CMS	Multi	FSFTASK2	(none)
IBM	VM/CMS	Multi	GCS	(none)
IBM	VM/CMS	Multi	IDMS	(none)
IBM	VM/CMS	Multi	IDMSSE	(none)
IBM	VM/CMS	Multi	IIPS	(none)
IBM	VM/CMS	Multi	IPFSERV	(none)
IBM	VM/CMS	Multi	ISPVM	(none)
IBM	VM/CMS	Multi	IVPM1	(none)
IBM	VM/CMS	Multi	IVPM2	(none)
IBM	VM/CMS	Multi	MAINT	(none)
IBM	VM/CMS	Multi	MOESERV	(none)
IBM	VM/CMS	Multi	NEVIEW	(none)
IBM	VM/CMS	Multi	OLTSEP	(none)
IBM	VM/CMS	Multi	OP1	(none)
IBM	VM/CMS	Multi	OPERATNS	(none)
IBM	VM/CMS	Multi	OPERATOR	(none)
IBM	VM/CMS	Multi	PDMREMI	(none)
IBM	VM/CMS	Multi	PENG	(none)
IBM	VM/CMS	Multi	PROCAL	(none)
IBM	VM/CMS	Multi	PRODBM	(none)
IBM	VM/CMS	Multi	PROMAIL	(none)
IBM	VM/CMS	Multi	PSFMAINT	(none)
IBM	VM/CMS	Multi	PVM	(none)
IBM	VM/CMS	Multi	RDM470	(none)
IBM	VM/CMS	Multi	ROUTER	(none)
IBM	VM/CMS	Multi	RSCS	(none)
IBM	VM/CMS	Multi	RSCSV2	(none)
IBM	VM/CMS	Multi	SAVSYS	(none)
IBM	VM/CMS	Multi	SFCMI	(none)
IBM	VM/CMS	Multi	SFCNTRL	(none)
IBM	VM/CMS	Multi	SMART	(none)
IBM	VM/CMS	Multi	SQLDBA	(none)
IBM	VM/CMS	Multi	SQLUSER	(none)
IBM	VM/CMS	Multi	SYSADMIN	(none)
IBM	VM/CMS	Multi	SYSCKP	(none)
IBM	VM/CMS	Multi	SYSDUMP1	(none)
IBM	VM/CMS	Multi	SYSERR	(none)
IBM	VM/CMS	Multi	SYSWRM	(none)
IBM	VM/CMS	Multi	TDISK	(none)
IBM	VM/CMS	Multi	TEMP	(none)
IBM	VM/CMS	Multi	TSAFVM	(none)
IBM	VM/CMS	Multi	VASTEST	(none)
IBM	VM/CMS	Multi	VM3812	(none)
IBM	VM/CMS	Multi	VMARCH	(none)
IBM	VM/CMS	Multi	VMASMON	(none)

IBM	VM/CMS		Multi	VMASSYS	(none)	
IBM	VM/CMS		Multi	VMBACKUP	(none)	
IBM	VM/CMS		Multi	VMBSYSAD	(none)	
IBM	VM/CMS		Multi	VMMAP	(none)	
IBM	VM/CMS		Multi	VMTAPE	(none)	
IBM	VM/CMS		Multi	VMTLIBR	(none)	
IBM	VM/CMS		Multi	VMUTIL	(none)	
IBM	VM/CMS		Multi	VSEIPO	(none)	
IBM	VM/CMS		Multi	VSEMAINT	(none)	
IBM	VM/CMS		Multi	VSEMAN	(none)	
IBM	VM/CMS		Multi	VTAM	(none)	
IBM	VM/CMS		Multi	VTAMUSER	(none)	
Intel	Shiva		Multi	Guest	(none)	User
Intel	Shiva		Multi	root	(none)	Admin
Intel	Shiva Lanrovers		Multi	root	(none)	Admin
Intel	LanRover VPN Gateway	< 6.0	Multi	n/a	isolation	Admin
Intel	LanRover VPN Gateway	6.0 >	Multi	n/a	shiva	Admin
Interbase	Interbase Database Server	All	Multi	SYSDBA	masterkey	Admin
IRC	IRC Daemon		IRC	n/a	FOOBAR	Acess
Iwill	PC BIOS		Console	n/a	iwill	Admin
JD Edwards	WorldVision/OneWorld	All(?)	TCP 1964	JDE	JDE	Admin/SECOFR
Jetform	Jetform Design		HTTP	Jetform	(none)	Admin
JetWay	PC BIOS		Console	n/a	spooml	Admin
Joss Technology	PC BIOS		Console	n/a	57gbzb	Admin
Joss Technology	PC BIOS		Console	n/a	technolgi	Admin
Lantronics	Lantronics Terminal Server		TCP 7000	n/a	access	Admin
Lantronics	Lantronics Terminal Server		TCP 7000	n/a	system	Admin
Leading Edge	PC BIOS		Console	n/a	MASTER	Admin
Linksys	DSL		Telnet	n/a	admin	Admin
Linux	Slackware		Multi	gonzo	(none)	User
Linux	Slackware		Multi	satan	(none)	User
Linux	Slackware		Multi	snake	(none)	User
Linux	UCLinux for UCSIMM		Multi	root	uClinux	Admin
Livingston	IRX Router		Telnet	!root	(none)	
Livingston	Livingston Portmaster 3		Telnet	!root	(none)	
Livingston	Officerouter		Telnet	!root	(none)	
Lucent	System 75		Multi	bciim	bciimpw	
Lucent	System 75		Multi	bcim	bcimpw	
Lucent	System 75		Multi	bcms	bcmspw	
Lucent	System 75		Multi	bcms	bcmspw	
Lucent	System 75		Multi	bcnas	bcnaspw	
Lucent	System 75		Multi	blue	bluepw	
Lucent	System 75		Multi	browse	browsepw	
Lucent	System 75		Multi	browse	looker	
Lucent	System 75		Multi	craft	craft	
Lucent	System 75		Multi	craft	craftpw	
Lucent	System 75		Multi	craft	craftpw	
Lucent	System 75		Multi	cust	custpw	
Lucent	System 75		Multi	enquiry	enquirypw	
Lucent	System 75		Multi	field	support	
Lucent	System 75		Multi	inads	indspw	
Lucent	System 75		Multi	inads	indspw	
Lucent	System 75		Multi	inads	inads	
Lucent	System 75		Multi	init	initpw	

Lucent	System 75		Multi	locate	locatepw	
Lucent	System 75		Multi	maint	maintpw	
Lucent	System 75		Multi	maint	rwmaint	
Lucent	System 75		Multi	nms	nmspw	
Lucent	System 75		Multi	pw	pwpw	
Lucent	System 75		Multi	rcust	rcustpw	
Lucent	System 75		Multi	support	supportpw	
Lucent	System 75		Multi	sysadm	sysadmpw	
Lucent	System 75		Multi	sysadm	admpw	
Lucent	System 75		Multi	sysadm	syspw	
Lucent	System 75		Multi	tech	field	
M Technology	PC BIOS		Console	n/a	mMmM	Admin
MachSpeed	PC BIOS		Console	n/a	sp99dd	Admin
Magic-Pro	PC BIOS		Console	n/a	prost	Admin
Megastar	PC BIOS		Console	n/a	star	Admin
Mentec	Micro/RSX		Multi	MICRO	RSX	Admin
Micron	PC BIOS		Console	n/a	sldkj754	Admin
Micron	PC BIOS		Console	n/a	xyzall	Admin
Micronics	PC BIOS		Console	n/a	dn_04rjc	Admin
Microplex	Print Server		Telnet	root	root	Admin
Microsoft	Windows NT		Multi	(null)	(none)	User
Microsoft	Windows NT		Multi	Administrator	Administrator	Admin
Microsoft	Windows NT		Multi	Administrator	(none)	Admin
Microsoft	Windows NT		Multi	Guest	Guest	User
Microsoft	Windows NT		Multi	Guest	(none)	User
Microsoft	Windows NT		Multi	IS_$hostname	(same)	User
Microsoft	Windows NT		Multi	User	User	User
Mintel	Mintel PBX			n/a	SYSTEM	Admin
Motorola	Cablerouter		Telnet	cablecom	router	Admin
MySQL	MySQL		all versions	root	(none)	Admin
NCR	NCR UNIX		Multi	ncrm	ncrm	Admin
NetGenesis	NetAnalysis Web Reporting		HTTP	naadmin	naadmin	Admin
Netopia	Netopia 7100		Telnet	(none)	(none)	Admin
Netopia	Netopia 9500		Telnet	netopia	netopia	Admin
NetworkICE	ICECap Manager	2.0.22 <	8081	iceman	(none)	Admin
NeXT	NeXTStep		Multi	me	(none)	User
NeXT	NeXTStep		Multi	root	NeXT	Admin
NeXT	NeXTStep		Multi	signa	signa	User
Nimble	PC BIOS		Console	n/a	xdfk9874t3	Admin
Nortel	Accelar (Passport) 1000 series routing switches		Multi	l2	l2	Layer 2 Read Write
Nortel	Accelar (Passport) 1000 series routing switches		Multi	l3	l3	Layer 3 (and layer 2) Read Write
Nortel	Accelar (Passport) 1000 series routing switches		Multi	ro	ro	Read Only
Nortel	Accelar (Passport) 1000 series routing switches		Multi	rw	rw	Read Write
Nortel	Accelar (Passport) 1000 series routing switches		Multi	rwa	rwa	Read Write All
Nortel	Extranet Switches		Multi	admin	setup	Admin
Nortel	Meridian PBX		Serial	login	0000	
Nortel	Meridian PBX		Serial	spcl	0000	
Nortel	Remote Office 9150		Client	admin	root	Admin
Novell	Netware		Multi	ADMIN	ADMIN	
Novell	Netware		Multi	ADMIN	(none)	
Novell	Netware		Multi	ARCHIVIST	(none)	

Novell	Netware	Multi	ARCHIVIST	ARCHIVIST
Novell	Netware	Multi	BACKUP	(none)
Novell	Netware	Multi	BACKUP	BACKUP
Novell	Netware	Multi	CHEY_ARCHSVR	CHEY_ARCHSVR
Novell	Netware	Multi	CHEY_ARCHSVR	(none)
Novell	Netware	Multi	FAX	FAX
Novell	Netware	Multi	FAX	(none)
Novell	Netware	Multi	FAXUSER	FAXUSER
Novell	Netware	Multi	FAXUSER	(none)
Novell	Netware	Multi	FAXWORKS	(none)
Novell	Netware	Multi	FAXWORKS	FAXWORKS
Novell	Netware	Multi	GATEWAY	GATEWAY
Novell	Netware	Multi	GATEWAY	GATEWAY
Novell	Netware	Multi	GATEWAY	(none)
Novell	Netware	Multi	GUEST	TSEUG
Novell	Netware	Multi	GUEST	GUESTGUEST
Novell	Netware	Multi	GUEST	GUESTGUE
Novell	Netware	Multi	GUEST	GUEST
Novell	Netware	Multi	GUEST	(none)
Novell	Netware	Multi	HPLASER	(none)
Novell	Netware	Multi	HPLASER	HPLASER
Novell	Netware	Multi	LASER	(none)
Novell	Netware	Multi	LASER	LASER
Novell	Netware	Multi	LASERWRITER	LASERWRITER
Novell	Netware	Multi	LASERWRITER	(none)
Novell	Netware	Multi	MAIL	(none)
Novell	Netware	Multi	MAIL	MAIL
Novell	Netware	Multi	POST	(none)
Novell	Netware	Multi	POST	POST
Novell	Netware	Multi	PRINT	(none)
Novell	Netware	Multi	PRINT	PRINT
Novell	Netware	Multi	PRINTER	(none)
Novell	Netware	Multi	PRINTER	PRINTER
Novell	Netware	Multi	ROOT	(none)
Novell	Netware	Multi	ROOT	ROOT
Novell	Netware	Multi	ROUTER	(none)
Novell	Netware	Multi	SABRE	(none)
Novell	Netware	Multi	SUPERVISOR	NETFRAME
Novell	Netware	Multi	SUPERVISOR	NFI
Novell	Netware	Multi	SUPERVISOR	NF
Novell	Netware	Multi	SUPERVISOR	HARRIS
Novell	Netware	Multi	SUPERVISOR	SUPERVISOR
Novell	Netware	Multi	SUPERVISOR	(none)
Novell	Netware	Multi	SUPERVISOR	SYSTEM
Novell	Netware	Multi	TEST	TEST
Novell	Netware	Multi	TEST	(none)
Novell	Netware	Multi	USER_TEMPLATE	(none)
Novell	Netware	Multi	USER_TEMPLATE	USER_TEMPLATE
Novell	Netware	Multi	WANGTEK	(none)
Novell	Netware	Multi	WANGTEK	WANGTEK
Novell	Netware	Multi	WINDOWS_PASSTHRU	WINDOWS_PASSTHRU

Novell	Netware		Multi	WINDOWS_PASSTHRU	(none)	
Novell	Netware		Multi	WINSABRE	SABRE	
Novell	Netware		Multi	WINSABRE	WINSABRE	
Nurit	PC BIOS		Console	$system	(none)	Admin
Oracle	Oracle RDBMS	7,8	Multi	ADAMS	WOOD	
Oracle	Oracle RDBMS	7,8	Multi	APPLSYS	APPLSYS	
Oracle	Oracle RDBMS	7,8	Multi	APPS	APPS	
Oracle	Oracle RDBMS	7,8	Multi	AURORA@ORB@UNAUTHENTICATED	INVALID	
Oracle	Oracle RDBMS	7,8	Multi	BLAKE	PAPER	
Oracle	Oracle RDBMS	7,8	Multi	CLARK	CLOTH	
Oracle	Oracle RDBMS	7,8	Multi	CTXDEMO	CTXDEMO	
Oracle	Oracle RDBMS	7,8	Multi	CTXSYS	CTXSYS	
Oracle	Oracle RDBMS	7,8	Multi	DBSNMP	DBSNMP	RESOURCE and CONNECT roles
Oracle	Oracle RDBMS	7,8	Multi	DEMO	DEMO	
Oracle	Oracle RDBMS	7,8	Multi	JONES	STEEL	
Oracle	Oracle RDBMS	7,8	Multi	MDSYS	MDSYS	
Oracle	Oracle RDBMS	7,8	Multi	NAMES	NAMES	
Oracle	Oracle RDBMS	7,8	Multi	ORDPLUGINS	ORDPLUGINS	
Oracle	Oracle RDBMS	7,8	Multi	OUTLN	OUTLN	
Oracle	Oracle RDBMS	7,8	Multi	RMAN	RMAN	
Oracle	Oracle RDBMS	7,8	Multi	SCOTT	TIGER	
Oracle	Oracle RDBMS	7,8	Multi	SYS	CHANGE_ON_INSTALL	DBA +
Oracle	Oracle RDBMS	7,8	Multi	SYSADM	SYSADM	
Oracle	Oracle RDBMS	7,8	Multi	SYSTEM	MANAGER	
Oracle	Oracle RDBMS	7,8	Multi	TRACESRV	TRACE	
Oracle	Personal Oracle	8	Multi	PO8	PO8	
Osicom	JETXPrint	1000E/B	Telnet	sysadm	sysadm	Admin
Osicom	JETXPrint	1000E/N	Telnet	sysadm	sysadm	Admin
Osicom	JETXPrint	1000T/N	Telnet	sysadm	sysadm	Admin
Osicom	JETXPrint	500 E/B	Telnet	sysadm	sysadm	Admin
Osicom	NETCommuter Remote Access Server		Telnet	debug	d.e.b.u.g	User
Osicom	NETCommuter Remote Access Server		Telnet	echo	echo	User
Osicom	NETCommuter Remote Access Server		Telnet	guest	guest	User
Osicom	NETCommuter Remote Access Server		Telnet	Manager	Manager	Admin
Osicom	NETCommuter Remote Access Server		Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	1500 E/B	Telnet	debug	d.e.b.u.g	User
Osicom	NETPrint	1000E/D	Telnet	debug	d.e.b.u.g	User
Osicom	NETPrint	1000E/NDS	Telnet	debug	d.e.b.u.g	User
Osicom	NETPrint	1500E/N	Telnet	debug	d.e.b.u.g	User
Osicom	NETPrint	2000E/N	Telnet	debug	d.e.b.u.g	User
Osicom	NETPrint	1500 E/B	Telnet	echo	echo	User
Osicom	NETPrint	1000E/D	Telnet	echo	echo	User
Osicom	NETPrint	1000E/NDS	Telnet	echo	echo	User
Osicom	NETPrint	1500E/N	Telnet	echo	echo	User
Osicom	NETPrint	2000E/N	Telnet	echo	echo	User
Osicom	NETPrint	1500 E/B	Telnet	guest	guest	User
Osicom	NETPrint	1000E/D	Telnet	guest	guest	User
Osicom	NETPrint	1000E/NDS	Telnet	guest	guest	User
Osicom	NETPrint	1500E/N	Telnet	guest	guest	User
Osicom	NETPrint	2000E/N	Telnet	guest	guest	User
Osicom	NETPrint	1500 E/B	Telnet	Manager	Manager	Admin

Osicom	NETPrint	1000E/D	Telnet	Manager	Manager	Admin
Osicom	NETPrint	1000E/NDS	Telnet	Manager	Manager	Admin
Osicom	NETPrint	1500E/N	Telnet	Manager	Manager	Admin
Osicom	NETPrint	2000E/N	Telnet	Manager	Manager	Admin
Osicom	NETPrint	1000E/NDS	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	1500E/N	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	2000E/N	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	1000E/B	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	2000E/B	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	1000E/N	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	2000E/N	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	1000 T/B	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	2000 T/B	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	1000 T/N	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	2000 T/N	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	1500 E/B	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	1500E/N	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	1500T/N	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	1000E/D	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	500 E/B	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	500 E/N	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	500 T/B	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	500 T/N	Telnet	sysadm	sysadm	Admin
Osicom	Osicom Plus T1/PLUS 56k		Telnet	write	private	
Packard Bell	PC BIOS		Console	n/a	bell9	Admin
Prime	PrimeOS		Multi	dos	dos	User
Prime	PrimeOS		Multi	guest	guest	User
Prime	PrimeOS		Multi	guest1	guest	User
Prime	PrimeOS		Multi	guest1	guest1	User
Prime	PrimeOS		Multi	fam	fam	User
Prime	PrimeOS		Multi	mail	mail	User
Prime	PrimeOS		Multi	maint	maint	User
Prime	PrimeOS		Multi	mfd	mfd	User
Prime	PrimeOS		Multi	netlink	netlink	User
Prime	PrimeOS		Multi	prime	prime	User
Prime	PrimeOS		Multi	prime	primeos	User
Prime	PrimeOS		Multi	primeos	prime	User
Prime	PrimeOS		Multi	primeos	primeos	User
Prime	PrimeOS		Multi	primenet	primenet	User
Prime	PrimeOS		Multi	primenet	primeos	User
Prime	PrimeOS		Multi	primos_cs	primos	User
Prime	PrimeOS		Multi	primos_cs	prime	User
Prime	PrimeOS		Multi	system	prime	Admin
Prime	PrimeOS		Multi	system	system	Admin
Prime	PrimeOS		Multi	tele	tele	User
Prime	PrimeOS		Multi	test	test	User
QDI	PC BIOS		Console	n/a	QDI	Admin
QDI	SpeedEasy BIOS		Console	n/a	lesarotl	Admin
Quantex	PC BIOS		Console	n/a	teX1	Admin
Quantex	PC BIOS		Console	n/a	xljlbj	Admin
Raidzone	raid arrays			n/a	raidzone	
Ramp Networks	WebRamp			wradmin	trancell	
RapidStream	RapidStream Appliances		Multi	rsadmin	(null)	Admin
Raritan	KVM Switches			admin	raritan	Admin

RedHat	Redhat 6.2		HTTP	piranha	q	User
RedHat	Redhat 6.2		HTTP	piranha	piranha	User
Remedy	Remedy		Multi	ARAdmin	AR#Admin#	Admin
Research	PC BIOS		Console	n/a	Col2ogro2	Admin
RM	RM Connect		Multi	admin	rmnetlm	
RM	RM Connect		Multi	admin2	changeme	
RM	RM Connect		Multi	adminstrator	changeme	
RM	RM Connect		Multi	deskalt	password	
RM	RM Connect		Multi	deskman	changeme	
RM	RM Connect		Multi	desknorm	password	
RM	RM Connect		Multi	deskres	password	
RM	RM Connect		Multi	guest	(none)	
RM	RM Connect		Multi	replicator	replicator	
RM	RM Connect		Multi	RMUser1	password	
RM	RM Connect		Multi	setup	changeme	
RM	RM Connect		Multi	teacher	password	
RM	RM Connect		Multi	temp1	password	
RM	RM Connect		Multi	topicalt	password	
RM	RM Connect		Multi	topicnorm	password	
RM	RM Connect		Multi	topicres	password	
RM	Server BIOS		Console	n/a	RM	
Semaphore	PICK O/S			DESQUETOP		
Semaphore	PICK O/S			DS		
Semaphore	PICK O/S			DSA		
Semaphore	PICK O/S			PHANTOM		
Shuttle	PC BIOS			n/a	Spacve	Admin
Siemens	Hicom 100E PBX			31994	31994	
Siemens	Hicom 150E PBX			31994	31994	
Siemens	PhoneMail			poll	poll	
Siemens	PhoneMail			poll	tech	
Siemens	PhoneMail			sysadmin	sysadmin	
Siemens	PhoneMail			system	system	
Siemens	PhoneMail			system	field	
Siemens	PhoneMail			tech	tech	
Siemens	ROLM PBX			admin	pwp	
Siemens	ROLM PBX			eng	engineer	
Siemens	ROLM PBX			op	op	
Siemens	ROLM PBX			op	operator	
Siemens	ROLM PBX			su	super	
Siemens Nixdorf	PC BIOS		Console	n/a	SKY_FOX	Admin
Silicon Graphics	IRIX		Multi	4Dgifts	4Dgifts	Admin
Silicon Graphics	IRIX		Multi	4Dgifts	(none)	Admin
Silicon Graphics	IRIX		Multi	demos	(none)	Admin
Silicon Graphics	IRIX		Multi	Ezsetup	(none)	Admin
Silicon Graphics	IRIX		Multi	field	field	Admin
Silicon Graphics	IRIX	5.x, 6.x	Multi	guest	(none)	CLI, UID guest
Silicon Graphics	IRIX	5.x, 6.x	Multi	lp	(none)	CLI, UID lp
Silicon Graphics	IRIX		Multi	OutOfBox	(none)	Admin
Silicon Graphics	IRIX		Multi	tour	tour	Admin
Silicon Graphics	IRIX		Multi	tutor	(none)	Admin
Silicon Graphics	IRIX		Multi	tutor	tutor	Admin
Sovereign Hill	InQuery			Admin	shs	Admin
Sun	Sun E10000 System Service Processor		Multi	ssp	ssp	Admin
Sun	SunScreen	3.1 Lite	TCP 3852	admin	admin	Admin

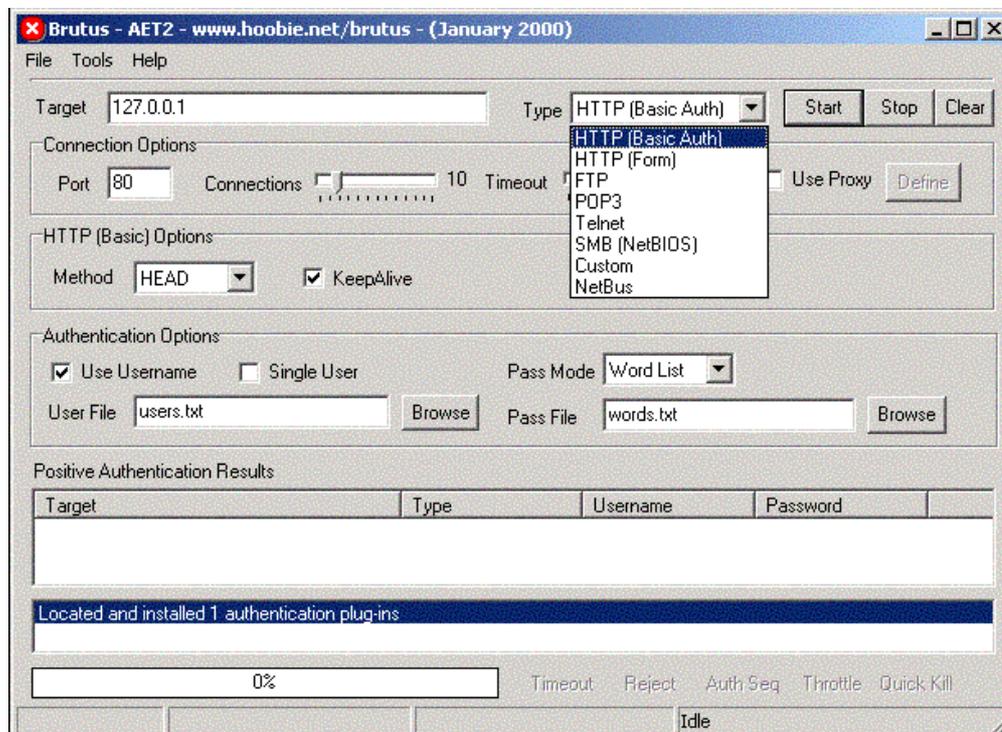
SuperMicro	PC BIOS		Console	n/a	ksdjfg934t	Admin
Sybase	Adaptive Server Enterprise	11.x,12.x	Multi	sa	(none)	SA and SSO roles
Telus	Telephony Services		Multi	(created)	telus00	User
Telus	Telephony Services		Multi	(created)	telus99	User
Tiny	PC BIOS		Console	n/a	Tiny	Admin
TMC	PC BIOS		Console	n/a	BIGO	Admin
Toshiba	PC BIOS		Console	n/a	24Banc81	Admin
Toshiba	PC BIOS		Console	n/a	Toshiba	Admin
Toshiba	PC BIOS		Console	n/a	toshy99	Admin
UNIX	Generic		Multi	adm	adm	Admin
UNIX	Generic		Multi	adm	(none)	Admin
UNIX	Generic		Multi	admin	admin	User
UNIX	Generic		Multi	administrator	administrator	User
UNIX	Generic		Multi	administrator	(none)	User
UNIX	Generic		Multi	anon	anon	User
UNIX	Generic		Multi	bbs	bbs	User
UNIX	Generic		Multi	bbs	(none)	User
UNIX	Generic		Multi	bin	sys	Admin
UNIX	Generic		Multi	bin	sys	Admin
UNIX	Generic		Multi	checkfs	checkfs	User
UNIX	Generic		Multi	checkfsys	checkfsys	User
UNIX	Generic		Multi	checksys	checksys	User
UNIX	Generic		Multi	daemon	daemon	User
UNIX	Generic		Multi	daemon	(none)	User
UNIX	Generic		Multi	demo	demo	User
UNIX	Generic		Multi	demo	(none)	User
UNIX	Generic		Multi	demos	demos	User
UNIX	Generic		Multi	demos	(none)	User
UNIX	Generic		Multi	dni	(none)	User
UNIX	Generic		Multi	dni	dni	User
UNIX	Generic		Multi	fal	(none)	User
UNIX	Generic		Multi	fal	fal	User
UNIX	Generic		Multi	fax	(none)	User
UNIX	Generic		Multi	fax	fax	User
UNIX	Generic		Multi	ftp	(none)	User
UNIX	Generic		Multi	ftp	ftp	User
UNIX	Generic		Multi	games	games	User
UNIX	Generic		Multi	games	(none)	User
UNIX	Generic		Multi	gopher	gopher	User
UNIX	Generic		Multi	gropher	(none)	User
UNIX	Generic		Multi	guest	guest	User
UNIX	Generic		Multi	guest	guestgue	User
UNIX	Generic		Multi	guest	(none)	User
UNIX	Generic		Multi	halt	halt	User
UNIX	Generic		Multi	halt	(none)	User
UNIX	Generic		Multi	informix	informix	User
UNIX	Generic		Multi	install	install	Admin
UNIX	Generic		Multi	lp	lp	User
UNIX	Generic		Multi	lp	bin	User
UNIX	Generic		Multi	lp	lineprin	User
UNIX	Generic		Multi	lp	(none)	User
UNIX	Generic		Multi	lpadm	lpadm	User
UNIX	Generic		Multi	lpadmin	lpadmin	User
UNIX	Generic		Multi	lynx	lynx	User

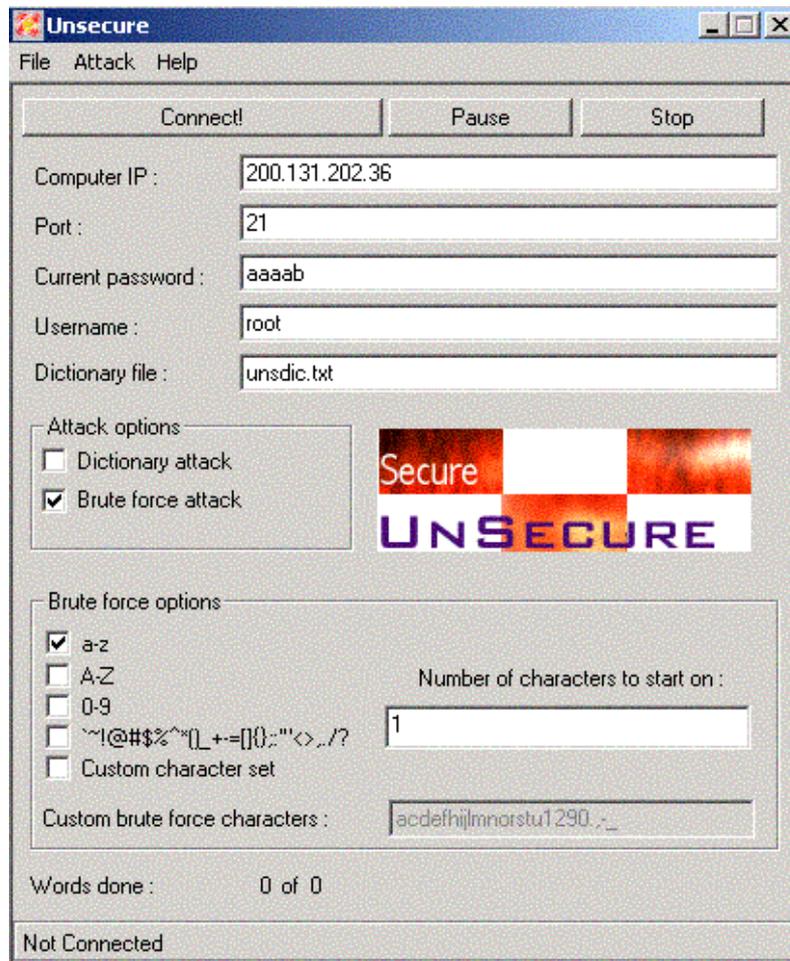
UNIX	Generic	Multi	lynx	(none)	User
UNIX	Generic	Multi	mail	(none)	User
UNIX	Generic	Multi	mail	mail	User
UNIX	Generic	Multi	man	man	User
UNIX	Generic	Multi	man	(none)	User
UNIX	Generic	Multi	me	(none)	User
UNIX	Generic	Multi	me	me	User
UNIX	Generic	Multi	mountfs	mountfs	Admin
UNIX	Generic	Multi	mountfsys	mountfsys	Admin
UNIX	Generic	Multi	mountsys	mountsys	Admin
UNIX	Generic	Multi	news	news	User
UNIX	Generic	Multi	news	(none)	User
UNIX	Generic	Multi	nobody	(none)	User
UNIX	Generic	Multi	nobody	nobody	User
UNIX	Generic	Multi	nuucp	(none)	User
UNIX	Generic	Multi	operator	operator	User
UNIX	Generic	Multi	operator	(none)	User
UNIX	Generic	Multi	oracle	(none)	User
UNIX	Generic	Multi	postmaster	postmast	User
UNIX	Generic	Multi	postmaster	(none)	User
UNIX	Generic	Multi	powerdown	powerdown	User
UNIX	Generic	Multi	rje	rje	User
UNIX	Generic	Multi	root	root	Admin
UNIX	Generic	Multi	root	(none)	Admin
UNIX	Generic	Multi	setup	setup	Admin
UNIX	Generic	Multi	shutdown	shutdown	User
UNIX	Generic	Multi	shutdown	(none)	User
UNIX	Generic	Multi	sync	sync	User
UNIX	Generic	Multi	sync	(none)	User
UNIX	Generic	Multi	sys	sys	Admin
UNIX	Generic	Multi	sys	system	Admin
UNIX	Generic	Multi	sys	bin	Admin
UNIX	Generic	Multi	sysadm	sysadm	Admin
UNIX	Generic	Multi	sysadm	admin	Admin
UNIX	Generic	Multi	sysadmin	sysadmin	Admin
UNIX	Generic	Multi	sysbin	sysbin	Admin
UNIX	Generic	Multi	system_admin	(none)	Admin
UNIX	Generic	Multi	system_admin	system_admin	Admin
UNIX	Generic	Multi	trouble	trouble	User
UNIX	Generic	Multi	umountfs	umountfs	User
UNIX	Generic	Multi	umountfsys	umountfsys	User
UNIX	Generic	Multi	umountsys	umountsys	User
UNIX	Generic	Multi	unix	unix	User
UNIX	Generic	Multi	user	user	User
UNIX	Generic	Multi	uucp	uucp	User
UNIX	Generic	Multi	uucpadm	uucpadm	User
UNIX	Generic	Multi	web	(none)	User
UNIX	Generic	Multi	web	web	User
UNIX	Generic	Multi	webmaster	webmaster	User
UNIX	Generic	Multi	webmaster	(none)	User
UNIX	Generic	Multi	www	(none)	User
UNIX	Generic	Multi	www	www	User
Unknown	System 88	Console	test	test	User
Unknown	System 88	Console	operator	operator	Admin

Unknown	System 88		Console	overseer	overseer	Admin
Unknown	POCSAG Radio Paging	2.05	Port 8000	n/a	password	Admin
Verifone	Verifone Junior	2.05		(none)	166816	
Vextrec Technology	PC BIOS		Console	n/a	Vextrex	
Vobis	PC BIOS		Console	n/a	merlin	Admin
Wim Bervoets	WIMBIOSnbsp BIOS		Console	n/a	Compleri	Admin
WWWBoard	WWWADMIN.PL		HTTP	WebAdmin	WebBoard	Admin
Xylan	Omniswitch		Telnet	admin	switch	Admin
Xylan	Omniswitch		Telnet	diag	switch	
Xyplex	Routers		Port 7000	n/a	access	User
Xyplex	Routers		Port 7000	n/a	system	Admin
Xyplex	Terminal Server		Port 7000	n/a	access	User
Xyplex	Terminal Server		Port 7000	n/a	system	Admin
Zenith	PC BIOS		Console	n/a	3098z	Admin
Zenith	PC BIOS		Console	n/a	Zenith	Admin
ZEOS	PC BIOS		Console	n/a	zeosx	Admin
Zyxel	Generic Routers		Telnet	n/a	1234	Admin

Multi-bruteforce

Existem muitos programas de bruteforce específicos, como o **WebCrack** (que quebra senhas de páginas web). Mas há também excelentes programas que conseguem quebrar senhas de vários tipos diferentes, como senhas de e-mai, netbios, web, unix, enfim, quase tudo. Já citei o **Shadow Scan**, mas mostrarei dois outros programas ótimos nessa tarefa:

Brutus: Excelente programas de bruteforce. Rápido e com uma configuração muito específica, produz excelentes resultados. Até senhas de netbus ele quebra. E salva as sessões.

Menu do programa Brutus

Unsecure: Mais rápido que o brutus, esse excelente bruteforce é um dos mais usados para o Windows. Sabendo a porta do servidor (ftp, telnet, etc...), o programa faz o serviço para você.

Programa Unsecure sendo usado

Política de senhas não-crackeáveis

Não existe mistério para que se possa ter uma senha segura. Se você utilizar o sistema Unix, crie uma combinação não-lógica de letras e números. Como por exemplo:

FqTp78nH

Apesar de ser mais difícil de se decorar do que senhas normais, a boa combinação dificulta muito que se consiga crackear a senha. Nunca coloque seu nome como senha, número de telefone, data de aniversário ou coisas assim. Seja precavido. Para Windows existe um outro método muito bom para senhas, a utilização dos caracteres alt. Para ler mais sobre eles, consulte o capítulo 12 (DOS).

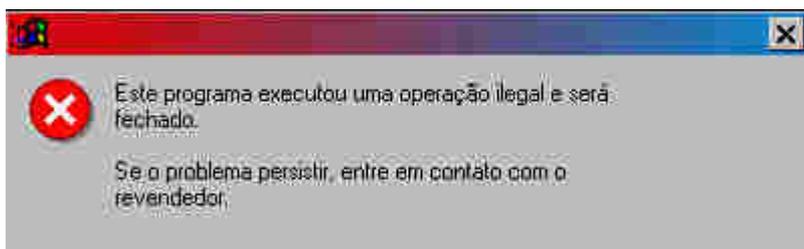
12

Falhas

Definição

Todos os sistemas têm falhas. Elas consistem em pequenos erros na criação dos programas, possibilitando que crackers os utilizem para tomar o controle de alguma máquina. Existem em absolutamente todo tipo de software, desde um simples tocador de mp3, um aparentemente inofensivo editor de texto, um jogo de computador e até mesmo o próprio sistema operacional. Essas falhas por mais insignificantes que pareçam, podem comprometer a segurança de uma rede inteira. E a maior de todas as falhas é o desinteresse dos muitos administradores de hoje que acham que o termo bug é algum desenho do Walt Disney.

Como surge o bug

O bug, ou falha, surge a partir do momento que o programador comete um erro. Ou seja, indiretamente é um erro humano que gera a falha nos programas. Por serem pequenos erros e não aqueles cabeludos que fazem o compilador até rir do programador, muitas vezes passam despercebidos e só são descobertos por algum hacker ou analista de segurança. Os erros do Windows, por exemplo. A grande maioria das falhas descobertas, são os próprios usuários que descobrem. Os criadores mesmo que têm o codigo-fonte e conhecem o programa como a palma da mão raríssimas vezes percebem algum erro. Para ser mais seguro, um programa têm que ser testado de todas as maneiras possíveis. Coisa que não fazem mais hoje.

Exemplo perfeito de falha : General Protection Fault.

Exemplos de falhas

Algumas falhas são tão bobas que é difícil de acreditar. Vou tomar como exemplo novamente o sistema Windows, pois de longe é o que possui mais falhas (claro, todas podem ser corrigidas). O Windows 98 possui muitos erros, mas três são interessantes. O primeiro é que não consegue executar nem abrir nenhum link com a url c:\con\con . Se você tentar ir em iniciar e executar, o sistema travará e mostrará a famosa tela azul. Os outros dois são do

netbios. O primeiro possibilita que você acesse o diretório system do Windows por um compartilhamento de impressora. É só mapear o compartilhamento padrão **printer$.** O último possibilita que se descubra a senha do netbios sabendo apenas o primeiro caractere. Por exemplo: coloco no disco C compartilhado a senha *herodes*. Se alguém tentar o primeiro h já consegue acesso à minha rede. O Windows 2000 também possui algumas falhas, como deixar o netbios ativo em sua instalação. Saindo um pouco dos sistemas operacionais, alguns programas também possuem falhas graves.

Erros de Active X possibilitam que ao visitar um site, o Internet Explorer instale um programa no seu computador e o execute sem que você perceba. Preocupa-se em não abrir anexos de e-mail? Erros no outlook fazem com que só de receber os e-mails os anexos sejam executados automaticamente. O Internet Information Server , servidor de homepages da Microsoft, possui erros graves. Unicode, RDS, existem muitos. Um mais recente é uma falha no printer .isapi , fazendo com que se consiga acesso ao Windows 2000 pelo IIS 5.0 . O sistema Unix possui muitas falhas também, como no sendmail (chamado de maior bug da terra) e no Apache, mas é mais fácil exemplificar usando o maravilhoso sistema de Bill Gates. Um truquezinho: abra o Word, digite a função =rand(100,100) e aperte enter. Boas risadas.

Buffer overflows

O buffer overflow é um ataque usado a muito tempo e que ainda será muito usado. Compreende em lotar os buffers (memória disponível para aplicativos) de um servidor e incluir na sua lista de processos algum programa tal como um keylogger ou um trojan. Todos os sistemas são vulneráveis a buffer overflows e a solução é a mesma, procurar se já existem correções existentes. Novos erros desse tipo surgem todo dia, até o XP já têm alguns. Se atualize sempre para não ficar para trás.

Um dos usos famosos do buffer overflow é o **telnet reverso**. Ele consiste em fazer a máquina alvo conectar-se a um servidor no computador do cracker, fornecendo-lhe um shell (prompt) de comando. O **netcat**, chamado de "canivete suíço do TCP/IP", é uma espécie de "super-telnet", pois realiza conexões por UDP, serve como servidor, entre outras tarefas. Ele é o mais utilizado para a realização do telnet reverso, e pode ser usado tanto na arquitetura NT quanto no Unix. A versão para Windows está disponível em ftp.technotronic.com .

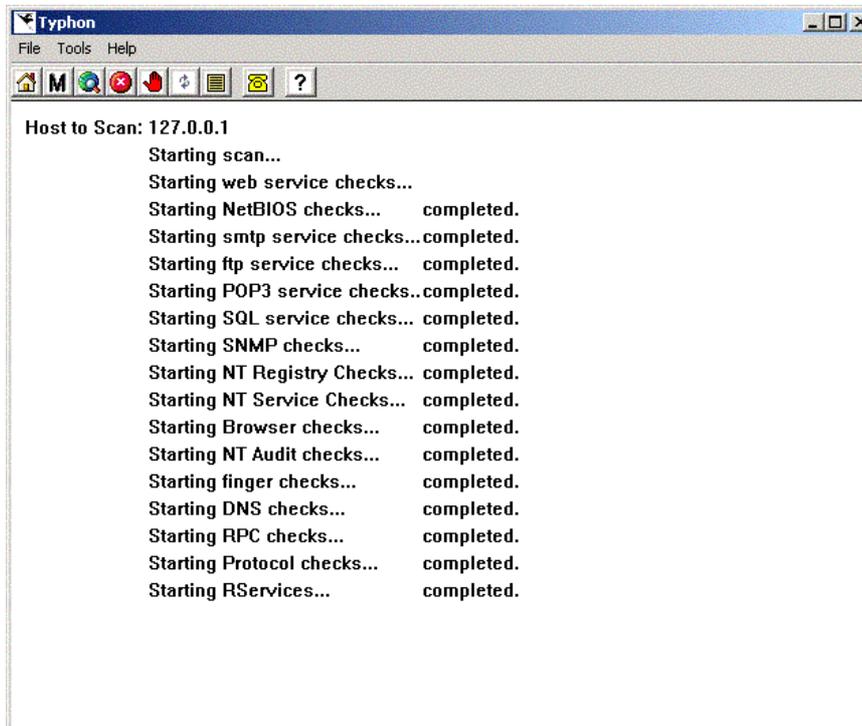
Race condition

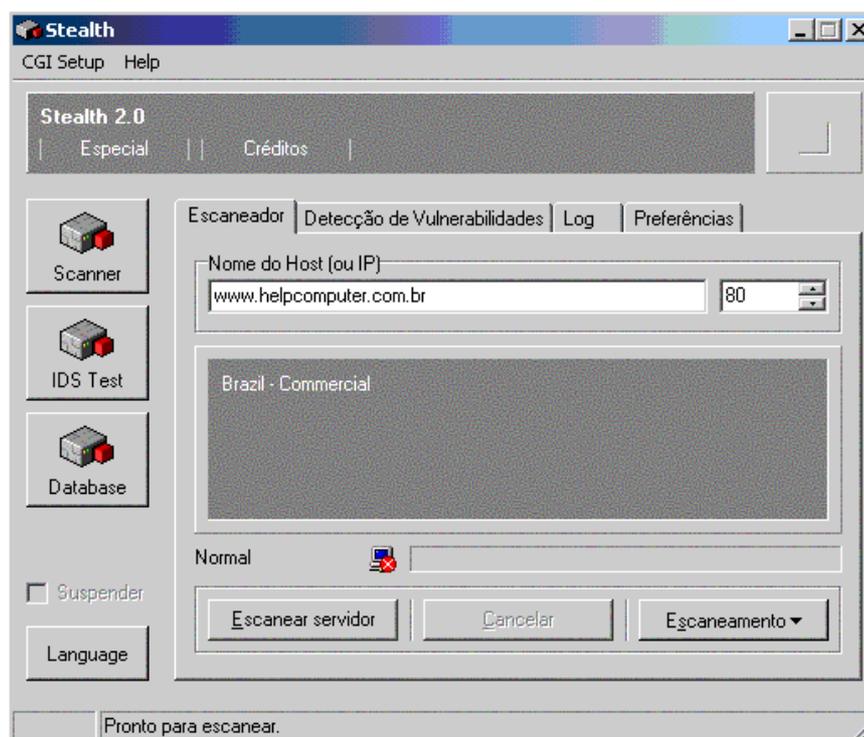
O Race condition ou condição de corrida é mais comum no Unix e no Linux. Consiste em fazer algum programa que rode como root (super-usuário) executar alguma falha que possa lhe enviar para o shell do sistema. O programa que mais teve problemas de race condition até hoje é o sendmail , serviço de e-mail padrão do Unix. É possível encontrar falhas até em versões mais recentes.

Descobrindo se algum sistema têm falhas

Para o programador experiente é mais fácil verificar se um sistema têm falhas (se o programador for interessado e tiver boa vontade), utilizando de recursos de debug que checam por erros de buffer overflow e outros. Para o usuário é bem mais difícil descobrir algo, principalmente o usuário comum. O interessante seria visitar páginas especializadas no assunto, que a cada dia publicam novos tipos de erros descobertos. Algumas muito boas são a Security-focus (**www.security-focus.com**) e a Hacker brasileira (www.hacker.com.br).

Anteriormente, na seção scanners, vimos alguns scanners de vulnerabilidade (ou falhas que dá na mesma). Veremos dois scanners melhores e mais potentes agora, o *Typhon* (**www.securityfocus.com**) e o *Stealth* **(www.nstalker.***com).*

- **Typhon** (Só funciona em Windows NT/2000/XP)

Esse scanner é excelente pois é rápido e nos dá algumas informações muito boas sobre possíveis falhas e desconfigurações do sistema alvo. Não é muito completo, mas é o ideal para se usar antes do magnífico **Stealth,** que como veremos, é inigualável**.**

- **Stealth**

O melhor scanner de vulnerabilidades do mundo. Isso é pouco para descrever o fantástico programa **Stealth**. Programa de uma empresa brasileira (e em português), ele já ganhou destaque internacional pois consegue identificar cerca de 15000 falhas em sistemas. Poucos conseguem escapar ilesos a essa potente arma. Portanto, use-a para o bem!

Utilizando exploits

Exploits são programas criados para explorar falhas. O exemplo do printer .isapi do IIS 5.0 que dei acima, possui um exploit chamado **iishack2000**.Ele possibilita que somente digitando o IP de algum computador, você consiga acesso direto ao interpretador de comandos (ou shell). Assim podendo fazer o que quiser com o sistema. Existe também o **iishack** (sem o 2000), que utiliza um erro de buffer overflow do IIS 4.0 para fazer com que você possa mandar o servidor executar qualquer tarefa (como um trojan). Cada exploit corresponde a uma falha, por isso geralmente os grandes sites de segurança publicam os dois juntos. Geralmente vêm em código-fonte C, Perl e alguns poucos em executáveis comuns. Se quiser encontrar compiladores para rodar os exploits, procure na página **www.programmersheaven.com**. É uma ótima homepage com muitos recursos de várias linguagens de programação. Se você não quiser arrumar um compilador, aí vai uma boa dica de exploit que checa mais de 200 vulnerabilidades de Unicode (IIS). Pegue em: **http://tomktech.n3.net**.

Instalando patches

Como já foi dito antes, a salvação está nos patches. Toda vez que um erro for descoberto, deve-se visitar a página do fabricante do programa e pegar a correção. Isso não pode ser feito de mês em mês, é no máximo de três em três dias. Os erros aparecem muito rápido, e um sistema é composto de muitos softwares. Todos devem ser checados. É interessante também assinar uma lista de discussão sobre segurança, assim toda vez que uma falha for descoberta, você receberá um e-mail. A Microsoft (www.microsoft.com), a Securenet (**www.securenet.com.br**) e Security-focus (www.securityfocus.com) possuem algumas.

13

Anonimidade

Ser anônimo na rede

Anonimidade na rede é algo muito discutido atualmente. Existe alguma maneira de ser totalmente indetectável na Internet? Existe sim e é bem simples. Muitos programas e ferramentas prometem tornar seu usuário invisível mas são pura enganação. O que você precisa é de conhecimento, não de softwares. Um usuário pode conseguir passar em computadores no Japão, Alemanha e Finlândia antes de atacar um site no Brasil. Aí que se faz a fama dos "metidos a crackers". Um cracker pega o seu notebook, vai a um telefone público, utiliza uma conta roubada de internet, se conecta a cinco computadores pelo mundo e utilizando-os conecta-se a um sistema de anonimidade. Após isso entra na página do FBI e apaga alguns arquivos. Nunca, digo nunca realmente com muito ênfase, será pego. Todos os bons crackers não são pegos, justamente pela facilidade de se esconder. Ou seja, não dependa de ferramentas de rastreamento, nem da polícia, nem nada. Apenas com a segurança do seu sistema. É a sua maior garantia.

Usando o anonymizer

O anonymizer é um dos muitos serviços gratuitos de anonimidade na net. Visitando a sua homepage (*www.anonymizer.com*) ele possibilita que você digite algum endereço e seja redirecionado para ele. Exemplo: eu digito *www.felainternet.com.br* na página do serviço e ele me redirecionará para o provedor de Internet FELA, só que com o endereço IP do anonymizer. Ou seja, se os administradores da página consultarem o log, não verão meu real endereço. Em sua versão básica (gratuita) o serviço possibilita apenas que você abra páginas HTTP. Ou seja, nada de FTP. Há ainda um serviço pago que pode ser conferido na página. Último detalhe: não é possível utilizar um anonymizer para conectar-se a outro.

Proxys

O proxy, antigo conhecido de muitas pessoas que mexem com rede, possibilita uma ponte entre um computador e um servidor. Para exemplificar melhor, imagine que você possui uma rede local, mas somente um dos seus computadores têm placa fax-modem. Então você se conecta por ele e utiliza um proxy para que o outro computador da rede faça uma ponte e acesse a Internet pelo servidor. O endereço IP utilizado será do servidor. Acontece que existem muitos proxys gratuitos na Internet. Brasileiros ou internacionais, eles possibilitam que você navegue tranqüilamente e às vezes ficam até mais rápidos do que com a conexão comum. O proxy também têm uma vantagem: você pode usar um proxy para entrar no

anonymizer (assim escondendo seu endereço IP duas vezes). Endereços gratuitos de proxy podem ser encontrados na página *www.cyberarmy.com.*

Wingates

O Wingate parece muito com o proxy, mas sua aplicação é um pouco mais perigosa por dois fatores. Primeiro: o wingate é acessado por telnet, então possibilita a conexão a qualquer tipo de servidores, sejam telnet, ftp, smtp, pop, ou até algum trojan. Segundo: ao contrário do anonymizer e do proxy que só pode ser usado uma vez, o wingate não têm limites. Você pode conectar-se a um wingate chinês, depois utilizá-lo para entrar em um argentino e um italiano. A cada conexão, você terá um novo endereço IP. Imagine o trabalho para algum administrador descobrir quem invadiu o sistema. Terá que entrar em contato com a autoridade de cada país e mesmo assim se ela quiser ajudar. É claro que a cada novo wingate a conexão vai ficando mais lenta. Só é bom mesmo para quem possui uma conexão de alta velocidade. Existem alguns scanners que procuram subnets por wingates. Alguns deles podem ser pegos em *ftp.technotronic.com*. Para uma lista de wingates, visite o site *www.cyberarmy.com*.

Remailers

O Remailer é muito parecido com os outros, mas é somente para se enviar e-mails anonimamente. Com ele não é preciso utilizar um wingate para se conectar a um servidor smtp, o próprio remailer já é um servidor anônimo. Mas por via das dúvidas, fique com o bom e velho wingate pois ele é mais garantido. Antes de sair mandando bombas de e-mail, saiba que esses serviços geralmente não conseguem manipular muitas mensagens em um pequeno intervalo. Isso quer dizer que qualquer um que dê uma de esperto e queira inundar a caixa de e-mails de outra pessoa com centenas de e-mails provavelmente vai ter o seu endereço IP real revelado.

Shells

Esse é realmente uma mão na roda. Uma vez alguém disse "O bom cracker não é o que consegue utilizar bem um sistema Unix e invadir uma rede. É o que utiliza Windows e consegue o mesmo resultado". Isso é uma verdade. Afinal, o Unix e o Linux podem até ser mais complicadinhos de se usar mas existem centenas de ótimas ferramentas para eles. É só pensar que quase todos os exploits disponíveis na Internet hoje são códigod-fonte em C. Já o Windows não possui tantos recursos assim, o que torna mais difícil alguma invasão usando esse sistema. Para facilitar existem os shells, máquinas utilizando serviços Unix na Internet que possibilitam que você se conecte nelas por telnet e ftp e as utilize como se fossem locais. Execute programas, compile códigos-fonte, utilize o bom e velho VI, use o sendmail e tudo o mais. Para uma lista de shells consulte a página *www.cyberarmy.com* ou cadastre-se no endereço *http://cyberspace.org/*.

Outdials

Citarei esse método mais como estudo pois ele é bem difícil de ser feito. O Outdial consiste em se conectar via telnet em algum sistema que possibilite conexão via modem. Deixe-me explicar melhor: você quer invadir um sistema nos EUA. Não têm dinheiro para se conectar diretamente (e pagar caro, apesar da prograganda das operadoras), então procura um outdial, se conecta via telnet e indica o telefone do sistema a ser invadido. O computador que roda o outdial discará e você conectará no sistema sem pagar absolutamente nada. O

problema é encontrar outdials hoje em dia. Não vai adiantar muito mas se quiser obter uma lista antiga de outdials, pegue o FAQ da 2600 em www.2600.com.

IP Spoof

A técnica mais antiga e devastadora de invasão de computadores. Trabalha a nível de protocolo, abaixo da camada dos aplicativos. É como o trojan de ponte, mas bem mais eficaz. No caso do trojan por exemplo, uma máquina era Windows, o que facilitou a sua instalação. Mas e uma rede que só existam máquinas Unix, mesmo assim fortemente seguras? Vamos supor que queremos invadir uma rede militar qualquer com 1000 computadores. O servidor central aonde ficam os dados confidenciais só se comunica com mais dois computadores, assim evitando o perigo de acesso pela Internet.

Ora, o erro está aí. Apesar de se comunicar só com duas máquinas, elas têm acesso à rede externa. Existe então uma *relação de confiança* entre esses computadores e o servidor. Aí que entra o IP SPOOF. Ele consiste em estudar com um sniffer as sequencias numéricas do cabeçalho ip que é enviado à maquina alvo. Supondo que a máquina alvo seja **A** (a que queremos invadir) e a que têm relação de confiança com ela seja **B**. Após aprender a sequência correta, inundamos a máquina **B** com pacotes syn malformados (criando um denial of service para “amordaçá-la”). Então criamos um pacote IP com cabeçalho falso, fingindo ser a máquina **B** (que não pode falar tadinha). Além disso, existem dois tipos de IP SPOOF.

Non-blind spoof

Esse spoof é realizado dentro da própria subnet em que se encontra o atacante. Ele é um spoof “não cego” pois permite que o atacante receba (usando um sniffer) a resposta da máquina A para a B após nosso ataque. Supondo que enviamos o comando:

< ip do hacker> >> /etc/rhosts

Esse é um comando para que o computador alvo passe a nos considerar “de confiança” , cedendo-nos espaço para quando fizermos um rlogin. Mas como saber se o comando funcionou? Com o non-blind spoof isso é possível.

Blind spoof

Quando o ataque é feito a um computador fora de sua subnet. Com o blind spoof, a única coisa que se pode fazer é enviar o pacote spoofado com o comando e rezar para funcionar. Um programa que automatiza um pouco a tarefa do spoof é o **SendIP** (www.earth.li) para Linux (Unix). Já para Windows não existe ainda um programa decente que o faça.

Sistemas operacionais

14

Unix e Linux

Como tudo começou

O UNIX foi desenvolvido na década de 70 pela Bell Labs. Seus criadores foram Ken Thompson e Dennis Ritchie, ajudados por uma equipe. O nome é uma gozação com o sistema Multics criado na década de 60 em que os dois se basearam. Enquanto ele tentava ser vários (Multi) o Unix era um só. Construiram um sistema operacional para programadores. Eles desejavam um resultado tão bom que a linguagem C foi desenvolvida só para ajudar a fazer melhores ferramentas para o projeto. A medida que o tempo foi passando, o UNIX foi se mostrando um sistema versátil e extremamente eficiente. Um pouco difícil para o usuário inexperiente, mas muito eficaz. Com esse sucesso todo, o sistema evoluiu e teve várias distribuições, tais como, Digital Unix, Aix, Unix V, Xenix, Minix e muitas outras. Também inspirou a criação de sistemas operacionais como o DOS e OS/2.

A sua mais famosa adaptação é o Linux, criado por Linus Torvalds (daí provém o seu nome). É uma distribuição gratuita (coisa que nem todos os unix são) e portada para os computadores pessoais já que geralmente os outros sistemas são para grandes computadores (mainframes). O sistema UNIX vêm se mantendo a mais de 30 anos como o sistema mais seguro e poderoso de todos.

Não entrarei em detalhes sobre o UNIX, já que esse livro não se prende a um sistema. Darei uma visão geral sobre como é sua estrutura e por quê difere tanto do Windows. O objetivo maior de um invasor em um sistema com UNIX é obter o acesso ROOT. Ele pode fazê-lo tentando explorar alguma falha em algum servidor da vítima (veja no capítulo falhas), como falhas em algum servidor (ou mesmo de algum kernel antigo), uma má-configuração, ou instalar um backdoor. Não importa. Se o invasor não conseguir acesso root ele não têm nada. E com certeza fará de tudo para conseguí-lo.

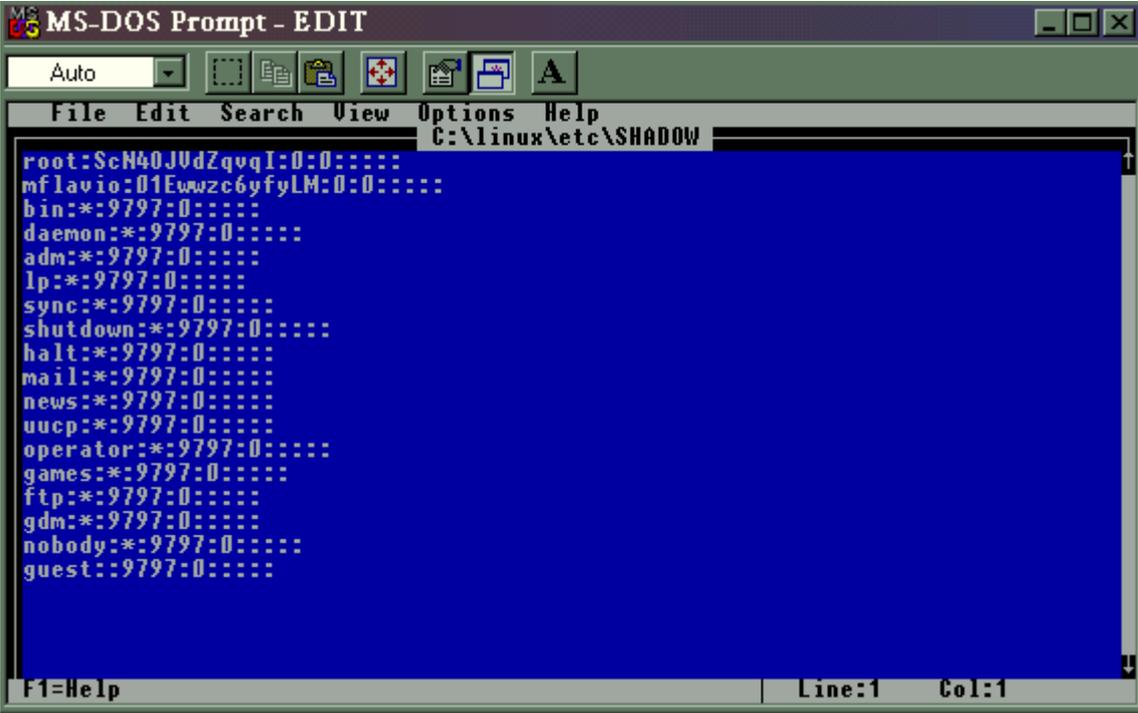
Autenticação de senhas – a criptografia DES

Sempre ao iniciar uma sessão, o sistema irá pedir-lhe nome de usuário e senha. Mas onde ficam armazenados esses dados?. O arquivo **/etc/passwd** é o responsável por guardar as senhas no sistema. O processo de autenticação no UNIX é extremamente eficiente. Aqui um exemplo simples de como o arquivo se organiza:

mflavio : Marcos Flávio :0 : 0: sEdkiUnbgFsbgTrVbgtTrfvfR : / : /bin/sh

A primeira seção é o login do usuário, no caso do exemplo é o **mflavio**. Esse é o nome usado para acesso ao sistema. Logo depois vemos o nome completo do usuário, que é **Marcos Flávio**. Depois vêm dois números. Eles são os números de indentificação de usuário e grupo. Os chamados IDs. No UNIX cada usuário pertence a um grupo, seja ele o root (administradores) , webmasters, users, o que for. Quanto menor for o número que aparece no arquivo passwd , maior é o poder do usuário. No exemplo temos dois zeros, isso quer dizer que o usuário têm poderes de administrador e pertence ao grupo root. Se fosse um usuário comum, provavelmente o número estaria entre 20 e 60.

A próxima seção é a mais interessante: a senha. Mas não a senha real, como é escrita ao se logar no sistema. Ela está criptografada usando um sistema chamado DES, desenvolvido especialmente para o UNIX. Contrariando alguns pensamentos, o DES não pode ser descriptografado. Mas ainda assim existem métodos para conseguir obter as senhas. Leia sobre ele no capítulo 14. Depois da senha criptografada temos o diretório padrão do usuário (que no caso do root é a raiz "/") e seu interpretador de comandos ou shell (/bin/sh). Existem outros shells, como o shell C (/bin/csh). A utilização de cada um depende do gosto do usuário.

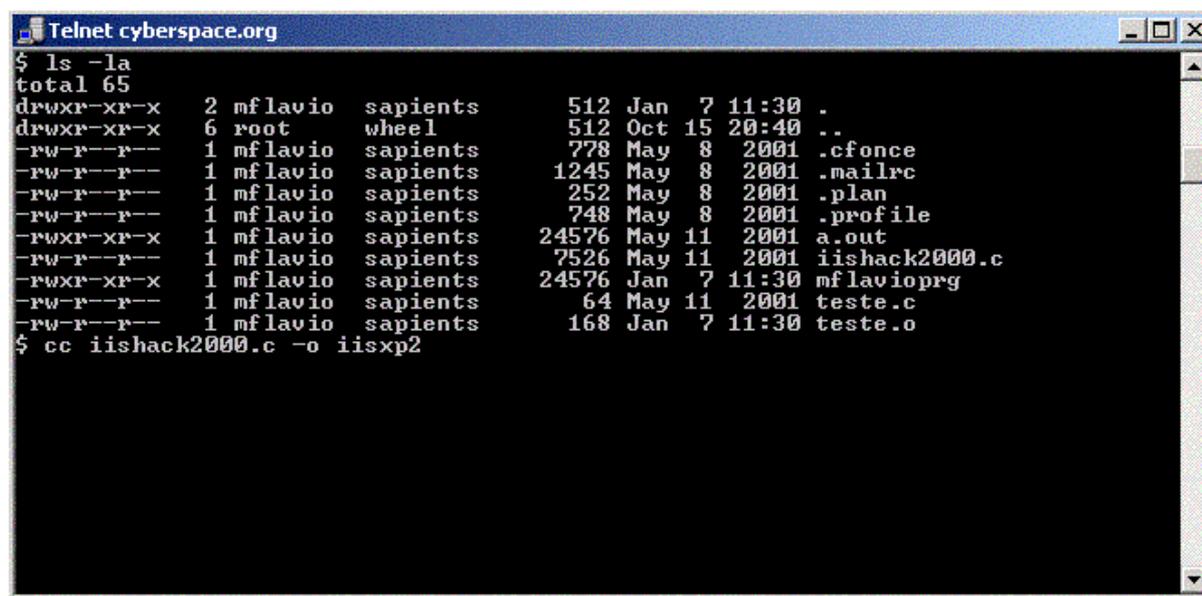
Uma observação interessante: em versões mais antigas do unix, usava-se o comando ln (que cria um link com algum arquivo) para criar um link com o arquivo de senha, mas agora acessível. Essa falha não mais existe. Seria mais ou menos assim: ln –l /etc/passwd /temp/teste . Isso faria que no diretório temp, existisse um link teste que poderia ser "acessado".

Um exemplo de arquivo de senha simples.

Shadowing

Na tentativa de segurar os invasores e impedir que consigam informações sobre o sistema, foi criado o sistema de Shadowing. Ele funciona da seguinte maneira: deixa-se um arquivo /etc/passwd “falso” para ser pego pelo cracker. Nesse arquivo, geralmente no lugar das senhas criptografadas estará apenas um asterisco. Os administradores mais maldosos que querem ver o invasor perder seu tempo, colocam algumas entradas criptografadas falsas de senhas. O arquivo verdadeiro está bem guardado em algum lugar do sistema. Como isso varia de sistema a sistema e o local pode ser modificado, teriam que procurar muito para encontrá-lo. É uma medida de segurança a mais, mas ainda assim não segura um bom cracker, que nem necessita do arquivo de senhas mais. Explora os erros.

SSH, Telnet e Rlogin

Os métodos de conexão remota são muito utilizados em sistemas UNIX. O Telnet e o Rlogin (remote login) por décadas foram largamente usados para que recursos externos distantes pudessem ser acessados. É como o patrão que de casa quer efetuar um login no sistema da empresa e verificar os logs para ver se está tudo bem. Acontece que após a popularização do sniffer esses acessos remotos ficaram perigosos pois eles enviam dados a texto puro, sem nenhum tipo de criptografia. Esse problema foi resolvido com a criação do SSH (Secure Shell) que começa a criptografar mesmo antes do processo de login.

Hoje, o SSH têm sido usado demais nos sistemas Linux, até já vêm com algumas distribuições. O erro que algumas pessoas fazem é confiar demais na sua eficiência. Como qualquer outro programa, o Secure Shell possui bugs graves. Até muitos se for comparado com outros serviços como o Apache. Portanto se o que você quer é a segurança do sistema, esteja sempre atualizando o seu SSH.

```
Telnet cyberspace.org
$ ls -la
total 65
drwxr-xr-x   2 mflavio  sapients     512 Jan  7 11:30 .
drwxr-xr-x   6 root     wheel        512 Oct 15 20:40 ..
-rw-r--r--   1 mflavio  sapients     778 May  8  2001 .cfonce
-rw-r--r--   1 mflavio  sapients    1245 May  8  2001 .mailrc
-rw-r--r--   1 mflavio  sapients     252 May  8  2001 .plan
-rw-r--r--   1 mflavio  sapients     748 May  8  2001 .profile
-rwxr-xr-x   1 mflavio  sapients   24576 May 11  2001 a.out
-rw-r--r--   1 mflavio  sapients    7526 May 11  2001 iishack2000.c
-rwxr-xr-x   1 mflavio  sapients   24576 Jan  7 11:30 mflavioprg
-rw-r--r--   1 mflavio  sapients      64 May 11  2001 teste.c
-rw-r--r--   1 mflavio  sapients     168 Jan  7 11:30 teste.o
$ cc iishack2000.c -o iisxp2
```

Com o utilitário telnet, consegui acesso a um sistema Unix.

Vírus e trojans

Essa é uma vitória do Unix. A coisa mais rara da face da Terra (mais raro que ganhar sozinho três vezes seguidas na mega-sena) é aparecer algum vírus para esse sistema. Tanto

que as empresas criadores de anti-vírus iriam falir se fizessem versões exclusivas para Unix e Linux. Trojans também existem muito poucos, e esses só conseguem ser instalados com o poder de superusuário (ou ROOT). Se você quer se livrar de uma vez por todas de problemas bobos como vírus de macro(Melissa) , worms(Love Letter) e outros, venha pra o Unix. Não irá se arrepender.

Buffer overflows e condição de corrida

Leia o capítulo sobre falhas.

Aumentando a segurança do sistema

Para aumentar a segurança é o que chamamos de praxe: esteja sempre atualizando o seu sistema por patches encontrados, teste-o com ferramentas de crackers para saber se é vulnerável. Configure os serviços que vão iniciar com o sistema no /etc/inet.conf . Cheque as permissões e os logs do sistema todos os dias. Use o shadowing. Utilize um bom firewall. Confira se todas as senhas padrões estão desabilitadas. E o essencial: reze. É uma ótima ajuda atualmente.

15

Microsoft

Como tudo começou

A história da Microsoft é bem interessante e pode ser vista no filme "Piratas da Informática", produzido pela *TNT*. Bill Gates e Paul Allen estudavam em Harvard juntos. Um dia ficaram sabendo de um lançamento de um tipo de computador (desses que ainda funcionavam a base de perfurações de cartões) e se ofereceram para criar o seu sistema operacional. Estava criada a *Microsoft*. Pouco tempo depois, um revolucionário chamado Steve Jobs lançou o primeiro computador pessoal do mundo , o **Apple II**. A apresentação do produto foi em uma pequena feira de informática, em que Bill Gates estava presente. A *IBM* resolveu lançar um produto para concorrer com a *Apple* (empresa de Steve Jobs). Estava montado o projeto do **PC/XT** (vulgo 186). Só que não possuiam um sistema operacional. A Microsoft correu para a IBM e ofereceu o **Ms-Dos**. Só havia um problema. Eles não tinham um sistema para vender. Foi um blefe. Logo encontraram um programador que havia feito um sistema fácil de usar baseado no **Unix**, mas com muito menos comandos. Bill comprou-o por uma mixaria e revendeu por um preço absurdo.

Esse foi o início de sua grande fortuna. A briga Apple II e PC/XT continuou até que uma empresa chamada *XEROX* inventou o mouse e a tela gráfica. Steve Jobs logo gostou do que viu e utilizou esses recursos no seu mais novo computador **Macintosh**. Percebendo o perigo a Microsoft se ofereceu para trabalhar para a Apple, assim conseguiram três protótipos do Macintosh. Curiosamente a Microsoft lançou um produto quase igual ao sistema gráfico da Apple, chamado **Windows**. Steve Jobs perdeu o emprego e voltou anos depois à Apple, tendo agora Bill Gates como acionista. Os últimos lançamentos de sua empresa são o **IMac** e o **Cube**.

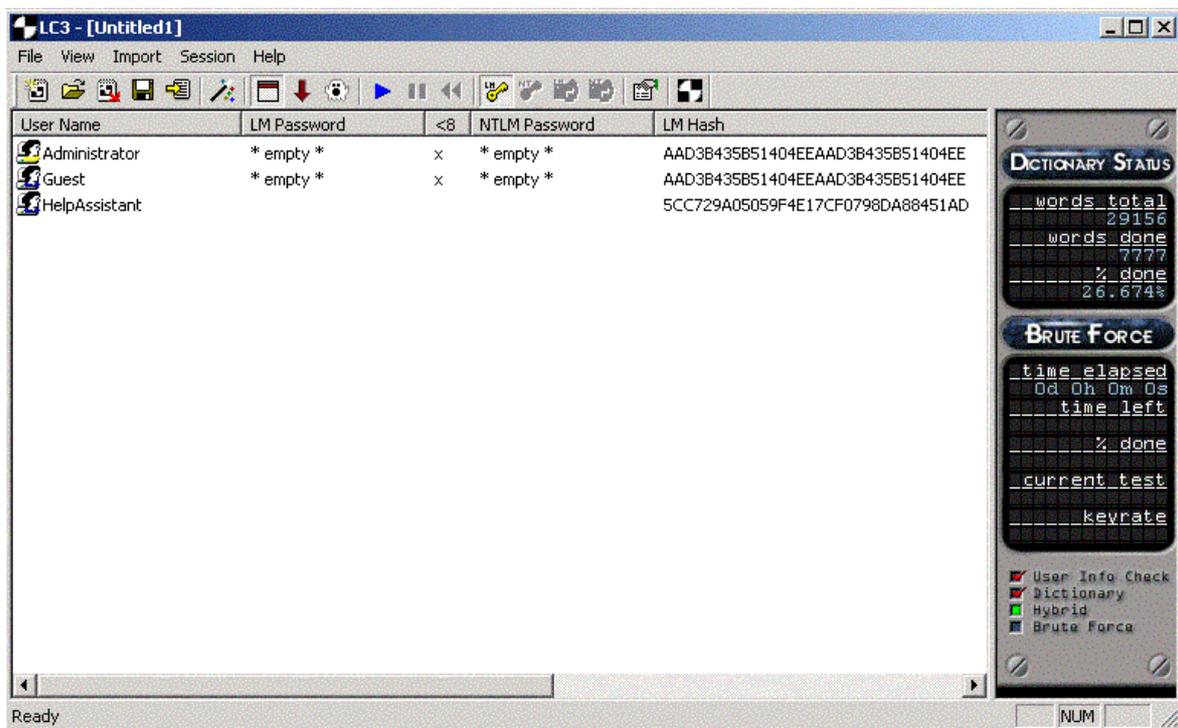
Diferenças das plataforma Windows ME e 2000

O Windows possui duas hierarquias. A primeira, vêm da sua primeira versão. Os mais antigos talvez se lembrem do **Windows 3.11** , aquele cheio das janelinhas. Pois é, depois dele vieram o **Windows 95**, o **98** e o **Millennium(ME)**. Essa hierarquia possui muitas falhas, algumas tão antigas que vêm do próprio DOS(falha do *con* por exemplo). Isso porquê a cada nova versão são acrescentadas novas tecnologias mas muitos erros não são corrigidos. Isso junta os antigos problemas aos novos. Quem nunca mexeu com o Windows e recebeu o famoso erro "Esse programa executou uma operação ilegal e será finalizado"? A Segunda hierarquia é a do Windows NT, atualmente chamado de Windows 2000. É infinitamente mais estável pois a cada nova versão o código-fonte é praticamente reescrito , portanto é um sistema para empresas. Para se ter idéia é raro dar algum erro no Windows NT, além de ele

possuir suporte a arquivos NTFS, o que deixa o sistema mais seguro. Um bom exemplo para mostrar a diferença entre as duas hierarquias, é o meu programa **Anti-Trojans**. Na sua versão **1.5** há mais de 50 opções de portas para serem monitoradas, mais quatro portas extras. No Windows 98 tentei abrir 25 portas e deu erro. Memória insuficiente. Ou quando abria, nada mais funcionava, o Internet Explorer não tinha memória para carregar mais nenhuma página. No Windows 2000, abri todas as portas ,inclusive as quatro as extras, e ainda abri o ICQ, o Netscape e o Napster. Por isso na versão **1.6**, diminuí o número de portas mas incluí um netstat.

A tentativa de se criar um sistema misturando elementos do Windows ME e do NT resultou no famoso Windows XP. Mas ele é apenas uma versão "mauricinha" do NT, já que a maioria dos programas mais antigos (principalmente os do 95,98 ou ME) acabam não rodando nele.

Autenticação de senhas

A autenticação no Windows NT é muito boa. Não tão quanto o Unix, claro. O processo é criptografado e oferece uma boa opção de segurança. Mas ao contrário do DES do Unix, pode ser quebrado mais facilmente. O excelente programa **LophtCrack** por exemplo, consegue descobrir senhas com uma velocidade fenomenal. E o NT (quando digo NT me refiro a todas as versões, inclusive o Windows 2000 que na verdade é o NT 5.0 e ao XP) não possui um recurso de shadowing, o que poderia ajudar a aumentar a segurança das senhas. Já a plataforma Windows 9x (atual ME) possui um método ridículo de autenticação de senhas. Na tela de login, só de você clicar em cancelar o sistema já inicializa. As senhas são gravadas em arquivos PWL no diretório do Windows, sendo super fáceis de serem quebrados. Muitos programas fazem isso, mas o **CAIN** é um dos melhores. É uma pena que ele não funcione no NT.

O LophtCrack consegue descobrir senhas do Windows NT localmente, em um sistema remoto (sendo admin) ou pela rede local como um sniffer. Ele tenta descobrir as senhas pelo LanMan, antigo algoritmo em que a autenticação do Windows NT se baseia.

Vírus e trojans

Michelângelo, Chernobil, Melissa, I Love You, várias gerações de um mesmo problema que atinge usuários do antigo DOS e do Windows por anos. Os malvados vírus. O que são exatamente os vírus? São programas em que a única função é causar danos ao computador, seja apagando arquivos, deixando a máquina mais lenta, etc. Em comparação a outros sistemas como o do Mac OS (Macintosh) ou o Unix, o Windows ganha de lavada na quantidade de vírus. Existem milhões e milhões de "bichinhos" para o Windows enquanto que para o Unix são apenas poucas dezenas. Vírus bobos (se é que podem ser chamados de vírus) como macros anexadas a documentos do office ou um arquivo vbscript têm causado muito pânico hoje em dia. Pense como as coisas são engraçadas: antigamente, quando se utilizava o DOS que é bem menos sofisticado e sem recursos, os vírus eram feitos por mestres da informática. Hackers e Crackers se utilizavam do assembler (linguagem de baixo nível) para criar seus vírus. E essa é uma linguagem bem mais difícil de ser aprendida que as comuns de alto nível (como basic, pascal, C, Perl e outras).

Hoje, com o Windows sendo altamente sofisticado, um simples arquivo VBScript causa muito estrago. Não precisa nem ser compilado e têm uma linguagem de programação extremamente fácil (baseado no Visal Basic). Infelizmente esse é o problema da geração Windows. Os que começaram seu aprendizado pelo DOS têm mais malícia em relação aos vírus. Para quem não conhece nada sobre esse antigo sistema, consulte o capítulo 12. A quantidade de trojans existente também é infinitamente maior no Windows que em outros sistemas. Como disse no início do livro, não existe um sistema melhor que o outro. Depende do seu uso e do gosto pessoal de cada um. Se utilizá-lo na empresa, use o Unix. Pelo menos os vírus não irão rondar seus sonhos à noite. Ou se preferir mesmo o Windows, arrume um bom anti-vírus (o **Norton** é um dos melhores). Eles ajudam muito.

Buffer overflows

Leia o capítulo sobre falhas.

Badwin

Badwin e Badcom são a mesma coisa, apenas um é para o sistema Windows e outro para o DOS. Podem ser feitos em Delphi ou VB e geralmente possuem comandos para apagar os arquivos do computador. Não podem ser considerados vírus ou trojans pois não ficam residentes na memória e nem são enviados pela rede (como os worms). Um badwin é um programinha extremamente simples, até mais do que os worms **vbscript**. Mas às vezes os programas são tão enfeitados (como aquele em que o botão corre) que as pessoas acabam caindo. E aí já é tarde.

Worms

Robert Morris Jr ficou famoso por ter criado o primeiro **worm** da história. Seu vírus especial conseguia atacar de rede em rede, causando danos enormes. E a diferença do vírus para o worm é essa: o worm é transmitido automaticamente pela rede, seja por e-mail, por ftp ou até por tcp/ip puro. Causa danos como o vírus, mas sua proporção é maior. Alguns

exemplos são o **Melissa** (worm de macro) e o **I Love You** (worm vbscript) que são enviados por e-mail. Os anti-vírus mais novos também costumam pegar os worms, mas infelizmente como não são programas compilados (executáveis) , são fáceis de serem alterados para enganar o software.

Aumentando a segurança do sistema

Use o Windows XP ou adote um Unix. Detesto puxar sardinha para algum sistema operacional mas ao escrever esse capítulo eu mesmo me convenci de que o Windows é um desastre da natureza de sistema operacional. Tive que reiniciar o computador umas vinte vezes em em pouco tempo. Muito fácil de se mexer, sem dúvida. E ótimo para joguinhos. Mas se você for precisar de um sistema sério , confiável e estável... use o MSX. (ei, isso foi uma piada). Como eu disse antes, é uma questão de gosto.

16

DOS

Por quê o DOS?

Ainda me recordo da primeira vez que o vi. Foi aos 10 anos, quando ganhei um 386. Fiquei maravilhado com toda aquela mágica de comandos. Expressões como **dir**, **cls** e **attrib** ainda faziam parte do nosso vocabulário. O **Qbasic** me possibilitou dar os meus primeiros passos em uma linguagem de programação. Era a época de grandes jogos como F1GP e Prince of Persia. É uma pena que o sistema operacional de disco (DOS) da Microsoft tende a não existir mais. A cada versão do Windows mata-se um pouco dele. No Millennium, nem é possível mais rodar alguns programas. Uma grande pena para os usuários da era do mouse.

Vemos pessoas assim chamar diretórios de pastas, copiar arquivos usando o Windows Explorer (sendo que não há nada melhor e mais gostoso de ser usado do que o comando copy do DOS). Recomendo sua aprendizagem a todos que não o conhecem. Vocês ainda têm tempo antes de adquirir um Windows XP chegar e acabar de assassinar nosso querido amigo. Foi em homenagem a ele que essa seção de dedica, mostrando truques e táticas de segurança.

Arquivos BAT

Os arquivos batch no DOS são pequenos scripts que possibilitam que se faça muitas tarefas de uma só vez. Possuem a extensão BAT e podem ser rodados como se fossem executáveis. A linguagem batch é bem extensa e ótima para iniciantes aprenderem os primeiros passos em programação. Meu objetivo não é ensinar a linguagem e sim apenas mostrar como o processo funciona. Um exemplo de um arquivo batch abaixo.

Dir/p

Cls

Mem

Digite no prompt do dos “edit teste.bat” . Assim o editor padrão EDIT irá criar o arquivo teste.bat . Escreva os três comandos acima, colocando-os um em cada linha. Salve o arquivo e execute-o digitando teste ou teste.bat . O programa listará os arquivos com pausa (dir/p), limpará a tela (cls) e mostrará o status da memória (mem).

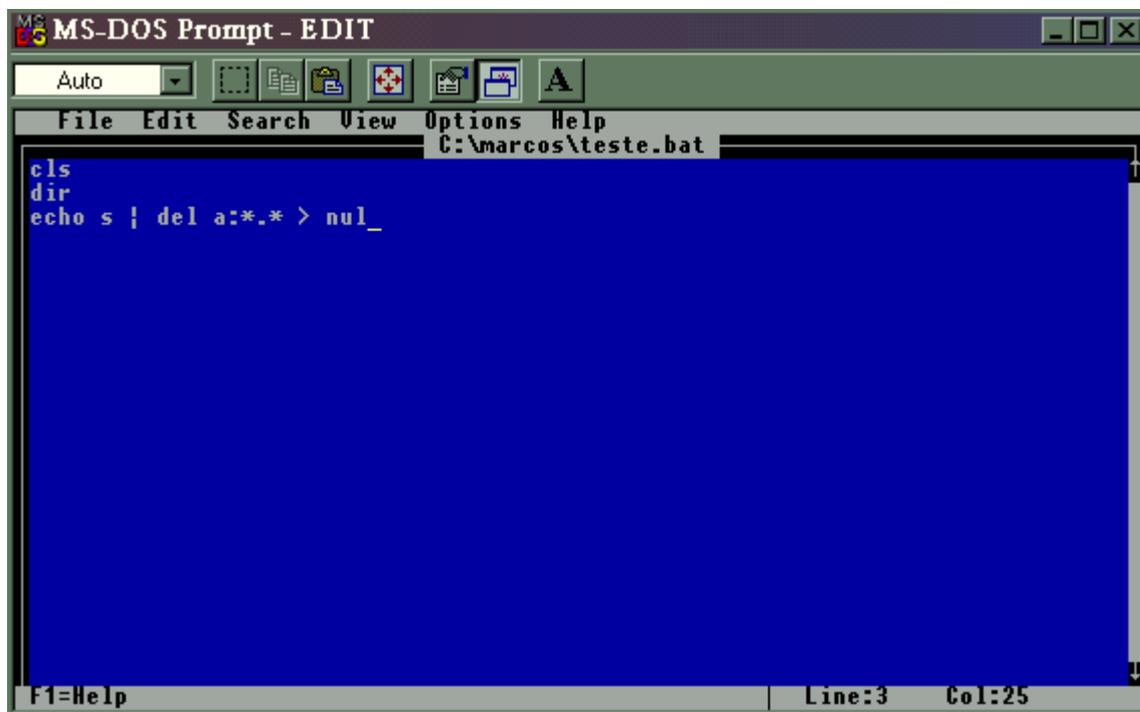
Badcoms

Os badcoms são uma má utilização de arquivos bat. Coloca-se no arquivo comandos destrutivos, tais como “del *.*” ou “deltree /y *.*” , que são comandos para apagar arquivos e diretórios. Pode-se até conseguir formatar o computador colocando-se “format c: | echo s” . O

pipe (|) fará com que o comando echo envie o caractere s para o comando format c:. Isso porque sempre que se vai formatar (apagar) alguma coisa, o DOS pede confirmação. No caso, o batch daria a confirmação por si próprio. Um exemplozinho rápido de um badcom:

Cls

@deltree /y *.* > nul

Ao criar esse arquivo BAT e executá-lo, o programa primeiro limpará a tela e logo depois usará o comando deltree para apagar os arquivos e pastas do computador. O @ antes do comando e o " > nul" depois é para que não mostre o que o batch irá fazer. Se você digitasse esse comando sem esses dois termos (somente deltree /y *.*), iria aparecer a mensagem "Excluindo <pasta ou arquivo> " . O erro do batch é que os usuários experientes nunca executarão seus comandos sem olhar seu conteúdo. Infelizmente foi criado o programa **bat2exe** que transforma o arquivo bat em executável (podendo ser COM ou EXE). Assim, muitas pessoas caem no seu truque a cada dia.

Nesse exemplo, enviamos o caractere s (echo s) para o comando del, assim ao executar o arquivo bat (ou badcom nesse caso) ele limpará a tela (cls), listará os dados(dir) e logo em seguida irá apagar o conteúdo do disquete (drive a). E ainda não mostrará nada na tela (nul).

Caracteres ALT

São obtidos ao se pressionar e segurar a tecla ALT e alguma sequência de três ou quatro números do keypad numérico (esse à direita do teclado). Alguns exemplos são ALT + 987 (que desenha um quadrinho amarelinho), ALT + 167 (símbolo º), ALT + 255 (caractere vazio, ótimo para criar arquivos sem nome) e muitos outros. Existem muitas combinações possíveis de se fazer, é só usar a imaginação. Os perigos dessa tática é criar diretórios usando caracteres ALT, assim o Windows não consegue acessá-los. Ou criar arquivos bem escondidos sem nome. Também têm as suas vantagens, se você criar uma senha com esses

caracteres, será extremamente mais difícil de ser descoberta. Pergunte ao seu provedor se o sistema deles admite o uso do ALT.

Primeiro criamos e acessamos um diretório usando caracteres ALT + 987 e ALT + 988.

Agora tentamos acessar o diretório criado pelo Windows Explorer.

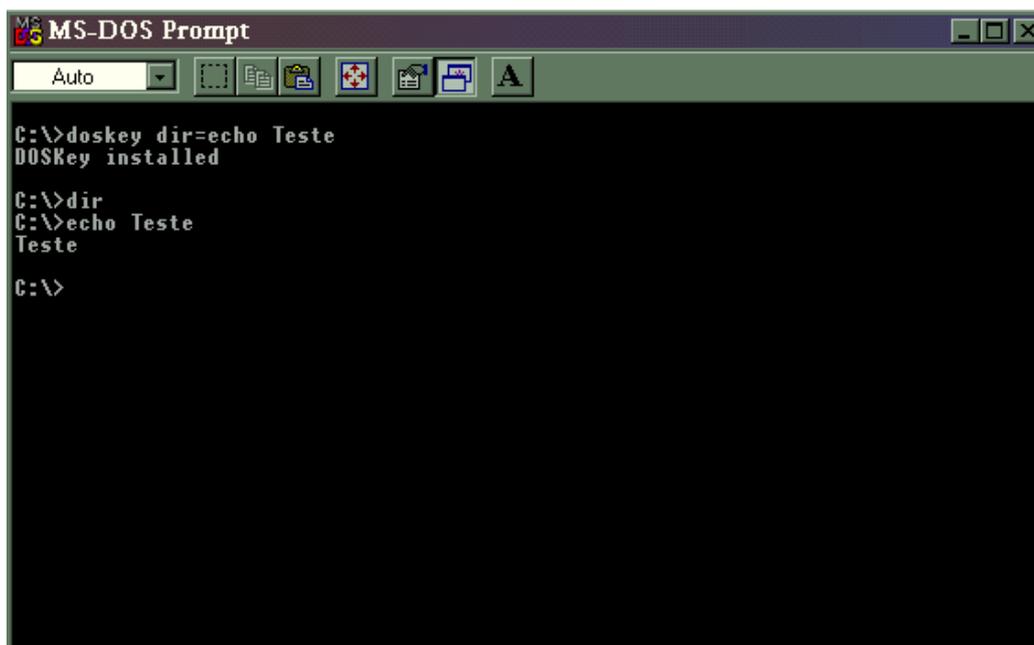
Macros do doskey

Os antigos usuários do DOS se lembram muito bem do nome doskey. Ele era muito utilizado para repetir os comandos mais usados pelo usuário ao se apertar a tecla para cima. Algo como o botão voltar do Internet Explorer. Mas esse pequeno comando pode ser utilizado para outros fins interessantes, como a criação de macros. Vamos fazer um teste criando uma macro chamada listar.

Doskey listar=dir

Ao executarmos a macro listar (executando-a como se fosse um comando comum), ela automaticamente dará um dir , ou seja, listará os diretórios e arquivos. Até aqui a coisa não têm muita graça. Mas e se utilizarmos os caracteres $T?

Doskey listar=dir/p $t mem

Neste exemplo, ao executarmos a macro listar o sistema dará um dir com pausa e executará logo em seguida o comando mem , que mostra o status da memória do sistema. Assim, usando o recurso $T podemos executar diversos comandos com uma só macro. Mas o interessante vêm agora:

Doskey dir = cls $t ver $t mem

Nós conseguimos criar uma macro com o próprio comando dir. Assim quando alguém for listar diretórios, tomará um susto danado. Isso funciona para todos os comandos do dos. Passe um bom susto em alguém. O exemplo a seguir mostra a criação de outra macro.

Para resetar as macros, aperte alt + f10.

Variáveis do sistema

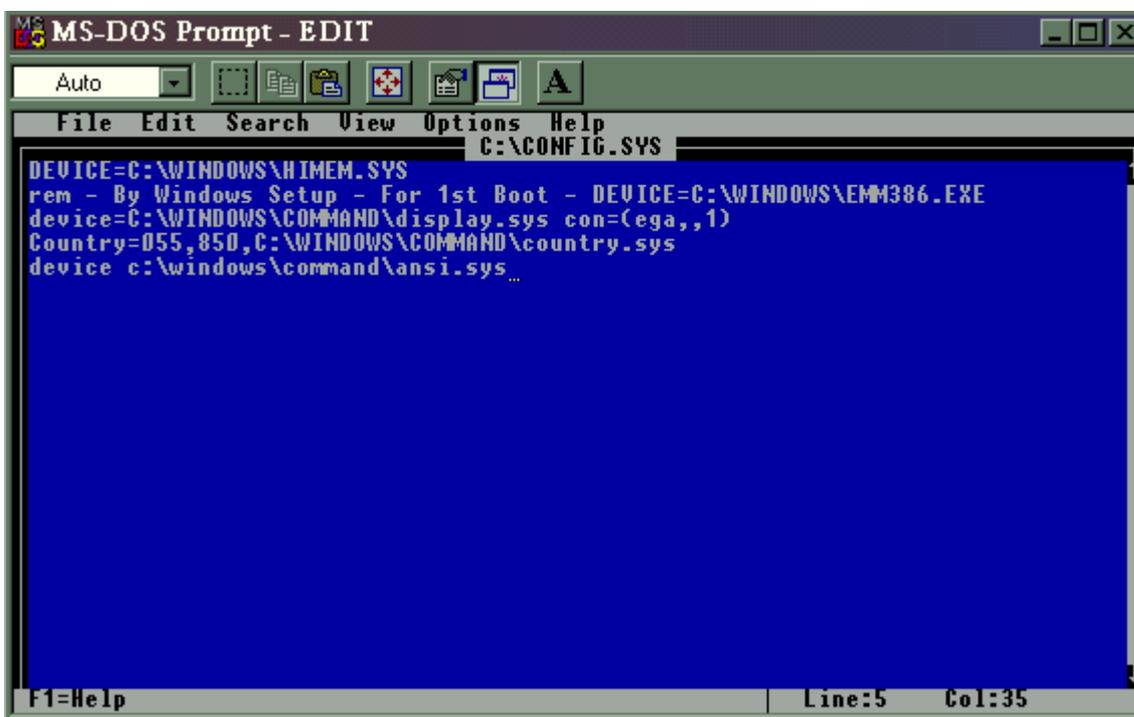
Vou abranger rapidamente essa seção dizendo apenas que existem muitas variáveis de sistema do DOS, e que todas podem ser mudadas usando o comand **set**. Vou demonstrar um ótimo exemplo:

Set dircmd=@

Isso fará com que ao listar os diretórios e arquivos, não apareça nada. O significado do @ é esse, esconder. Mas você pode colocar como dircmd a opção /p ou /w ou alguma outra. Elas irão automatizar o processo de listar com pausa, etc. Se teve dúvidas, tente fazê-lo que irá entender.

Comandos ANSI

Esse é o mais interessante de todos. Antes de tudo, verifique se existe essa linha no seu config.sys (ele fica na raiz). Se não existir, inclua.

Device = c:\windows\command\ansi.sys

Agora resete o computador. Vá para o prompt do DOS depois que ele reiniciar.

Deixe-me explicar por partes: primeiro vamos definir algumas cores dos números:

0 – Preto

1 – Vermelho

2 – Verde

3 – Amarelo

4 – Azul

7 – Branco

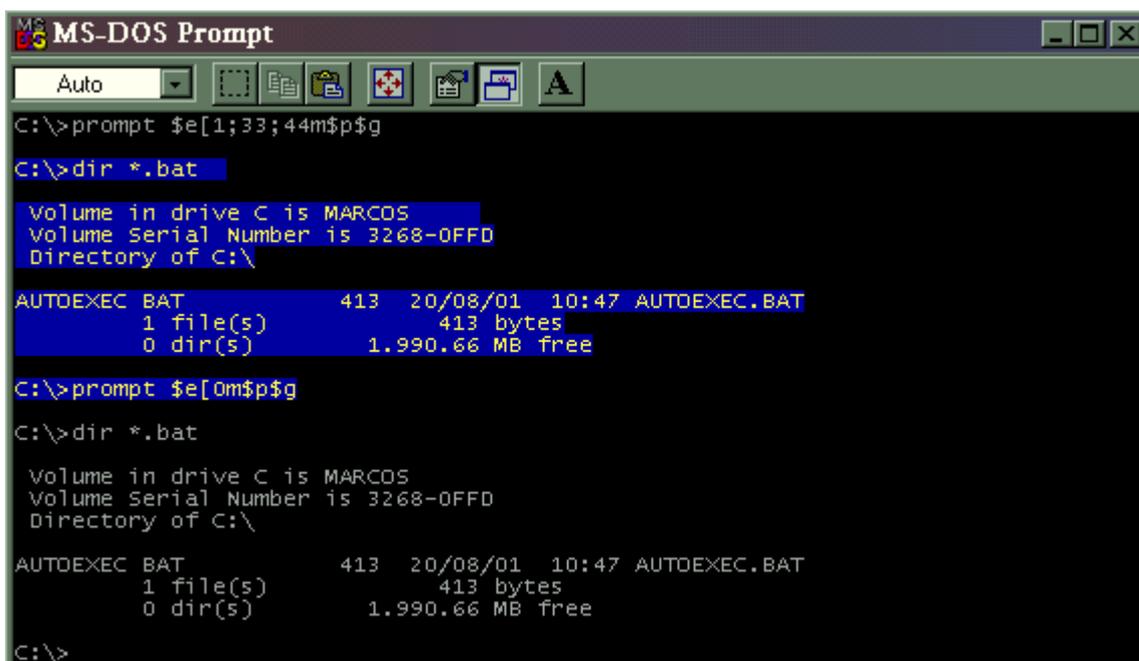
E agora o status:

0 – Letra mais forte

1 – Letra mais fraca

5 – Piscando

Ok, qual o significado de mostrarmos esses números? Você vai entender.

C:\> prompt $e[1;33;44m$p$g

```
MS-DOS Prompt
Auto
C:\>prompt $e[1;33;44m$p$g

C:\>dir *.bat

 Volume in drive C is MARCOS
 Volume Serial Number is 3268-0FFD
 Directory of C:\

AUTOEXEC BAT           413  20/08/01  10:47 AUTOEXEC.BAT
         1 file(s)             413 bytes
         0 dir(s)         1.990.66 MB free

C:\>prompt $e[0m$p$g

C:\>dir *.bat

 Volume in drive C is MARCOS
 Volume Serial Number is 3268-0FFD
 Directory of C:\

AUTOEXEC BAT           413  20/08/01  10:47 AUTOEXEC.BAT
         1 file(s)             413 bytes
         0 dir(s)         1.990.66 MB free

C:\>
```

O comando prompt (atenção, o c:\> não é para ser digitado) é usado para alterar esse c:\> do DOS. Mas a sua opção $e é a de ANSI. O exemplo acima é dividido em três partes: o número 1 é o status. Logo depois ele é separado da dezena de 30 pelo ponto e vírgula. A dezena de 30 é a responsável pela letra, então colocamos o 3 (ficando 33) para que a letra seja amarela. Logo depois outro ponto e vírgula separando a dezena de 40. E colocamos a cor azul (ficando 44).O **m** é usado para terminar a sentença e o pg são para o prompt continuar o mesmo (ou seja, não mudar o c:\>). Acho que já deu pra entender como se muda as cores, vamos mudar algumas teclas agora. Que tal o vírus cebolinha? Mudaremos a tecla r pela l.

C:\.> prompt $e[“r”;”l”p$p$g

Esse comando trocará a letra r pela l. Experimente pedir a alguém digitar seu nome. O **p** faz a mesma coisa que o **m** na cor. Mais dois exemplos apenas.

C:\> prompt $e[0;60;””;13p$p$g

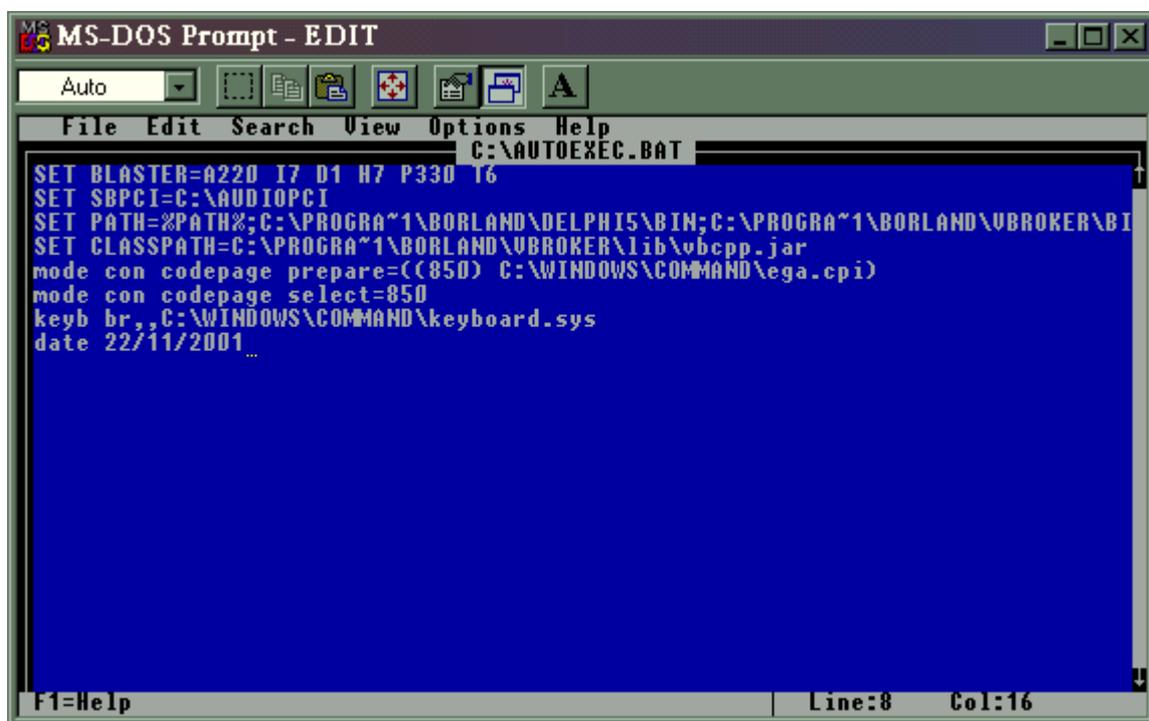
Esse comando transforma a tecla F2 (cujo código é 0;60) em Enter(o 13p no final). Agora vai o comando mais malvado de todos.

C:\> prompt $e[13;”deltree /y *.*”;13ppg

Cuidado ao executá-lo, ele fará com que só de pressionar a tecla Enter (código 13) , se execute o comando deltree /y *.* que apagará todos os arquivos. Troque o comando entre as aspas como teste. Para voltar as teclas ao normal, seria preciso saber o código delas. Há um método mais fácil. Feche o prompt do dos ou resete o computador.

Velhos truques

O DOS é cheio de truques muito interessantes. Vou dar apenas uma palhinha pois o gostoso é fuçar e descobrí-los por você mesmo. Mas tenho certeza de que essa dica será muito útil. Abra o arquivo autoexec.bat (que está na raiz) e coloque o comando date mais a sua data atual. Mais ou menos assim:

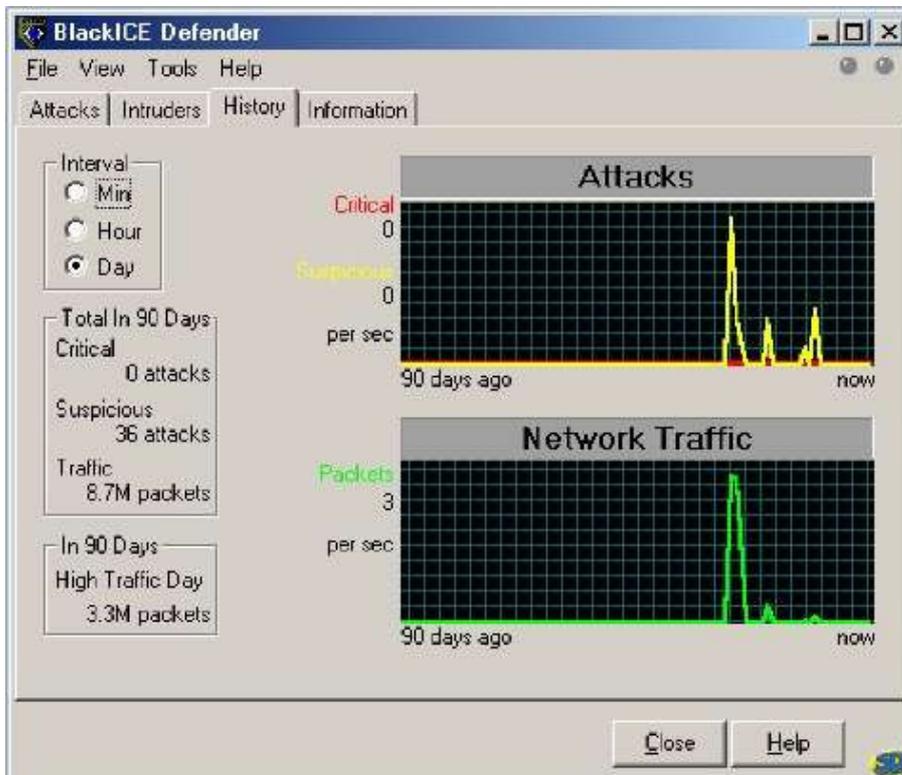
Date 22/11/2001

Salve o arquivo e resete o computador. Esse lhe trará duas vantagens: primeira: aqueles vírus com dias programados para atacar, nunca atacarão seu pc (e são mais de 50% dos vírus existentes) e segunda: os programas que você pode usar por 30 dias poderão ser usados para sempre. É uma ótima vantagem. Ah, os segredos do DOS **:-)**

Aprendendo a se proteger

17

Firewall

Conceito de Firewall

Firewall ou barreira de fogo é um artifício largamente usado em redes. A sua função é proteger o sistema de tentativas indevidas de acesso, principalmente vindas da Internet. Ele controla o tráfego, permitindo ou negando acesso a certas portas de serviços. Geralmente se deixa apenas a porta 80 (www) ativa para que as pessoas consigam acessar o website da empresa. Resumidamente o firewall é o seguinte: um HD que possui duas placas de rede, sendo uma ligada à rede corporativa e outra ligada à Internet. A partir disto pode-se implementar uma tentativa de segurança, que consiste em um pacote que determina o que é ou não permitido passar de uma rede à outra. Podem ser feitos de software ou hardware.

Exemplo do firewall blackice rodando. (www.blackice.com)

Eficiência

Existem 2 tipos de firewall: um que analisa a camada de rede, o pacote IP, e outro que analisa a camada de aplicação, dentro do pacote IP.

Firewall analizando a camada de rede

Estes se limitam ao nível de IP. Decidindo o destino dos pacotes (aceito ou não), tendo como base: remetente, porta IP utilizada e endereço do destinatário. Qualquer roteador pode ser configurado para firewall, mas será um firewall simples. Isto fará com que ele fique protegido contra crackers iniciantes, mas pode ser vítima de ataques comuns e bem clássicos. Como por exemplo: *o IP Spoof*

Em máquinas bem configuradas, a barreira de fogo concede acesso apenas a computadores considerados de confiança (endereços conhecidos). Para introduzir-se a uma máquina bem configurada é necessário fazer com que ela o considere confiável. Isto se chama spoofing. Consiste em mandar pacotes com o endereço legítimo de uma máquina da rede interna. A vítima acreditará que o invasor é de confiança e responderá enviando pacotes para o endereço do remetente. No entanto o cracker deve tomar precauções:

- **Certificar-se que a máquina legítima não responda aos pacotes. Isto é feito garantindo-se que ela esteja off-line(desconectada).**
- **Garantir que aqueles pacotes sejam enviados para a Internet, já que a máquina legítima encontra-se dentro da rede interna.**

Para isto é usado o "**source routing**", que consiste em uma técnica criada para testes. Ela permite que o computador que inicia a comunicação especifique qual a rota de todos os pacotes de uma certa conexão. Isto faz com que os pacotes sejam expelidos da rede pra a internet (veja em anonimidade uma explicação mais simples do IP Spoofing).

Firewalls mais novos não permitem a uso do spoofing e do souce-routing, pois eles, além de rotear os pacotes para seus destinos também mantém informações sobre o estado das conexões e sobre o conteúdo do pacote, o que permite impedir que um pacote pertencente à rede interna seja mandado à Internet. O firewall irá caracterizar isto como um ataque e tomará as devidas providências.

Sofisticados, ou não, eles são transparentes e rápidos pois roteiam tráfegos diretos e é exatamente isso que o impede de analizar o conteúdo efetivo do pacote e também exige que as máquinas na rede interna possuam um endereço IP válido.

Firewall analizando a camada de aplicação

Estes normalmente são CPUs de uso geral de rede que rodam programas chamados: "proxy servers" . Este tipo de firewall não permite comunicações diretas entre duas redes, pois requerem o estabelecimento de duas conexões. Uma delas do remetente proxy e a segunda entre o remetente e o destinatário. Todo pacote antes de ser ecoado é analizado pelo proxy server. Ele irá decidir se o pacote deve ou não ser descartado.

Vale saber que devido a estas caracteríscas o firewall de aplicação oferece uma segurança maior do que o firewall de rede, pois consegue perceber perigo em um pacote que o de rede não conseguiria.

Dois exemplos de coisas que este tipo de defesa pode filtrar são:

- O primeiro é DEBUG do SMTP que é usado para pedir a um servidor de correio que forneça algumas informações de controle. O que é considerado risco.

- Um segundo exemplo são os Proxys FTP, que vedam o acesso de usuários externos, mas mesmo assim, permite que os funcionários copiem arquivos da NET para a rede.

Cada uma dessas vantagens dependem do funcionamento do protocolo de defesa, sendo que estes não poderiam ser colocados nos firewalls de rede, já que não são capazes de analizar o conteúdo do pacote IP. Firewalls de rede são mais transparentes do que os de aplicação, já que os de aplicação exigem a existência de um proxy, além de proibir a comunicação direta entre o servidos e o cliente. É necessário que o programa cliente saiba que deve estabelecer com o proxy e determinar ações. Então basta configurar o browser corretamente.

Muitas vezes os clientes não são sofisticados o suficiente, e necessitam de conexões diretas com o servidor. Neste caso utiliza-se o seguinte artifício: o usuário se loga no proxy e este em vez de solicitar nome e senha (como seria de esperar), solicita o nome do servidor com o qual se deseja a conexão e a partir daí, tudo funciona normalmente.

Conclusão

Os firewalls são essenciais e importantíssimos, quando bem configurados. Possuem falhas (como visto anteriormente) assim como qualquer tipo de programa, e essas devem ser corrigidas. Nenhum firewall é 100% seguro, mas ajuda muito (ô como ajuda). Compre djá ! Ou use a nova moda fashion: soft livre. Cheque alguns firewalls em www.superdownloads.com.br (o pessoal do superdownloads têm que me agradecer, o link deles mais aparece aqui do que tudo). Experimente alguns como o **Conseal PC Firewall**, o **Zone Alarm** e outros.

Atenção: não sei se ficou bem claro mas o Firewall também pode ser usado muito bem contra trojans, pegando praticamente tudo (mas ele não retira o trojan do PC).

18

Códigos-fonte

A importância da programação

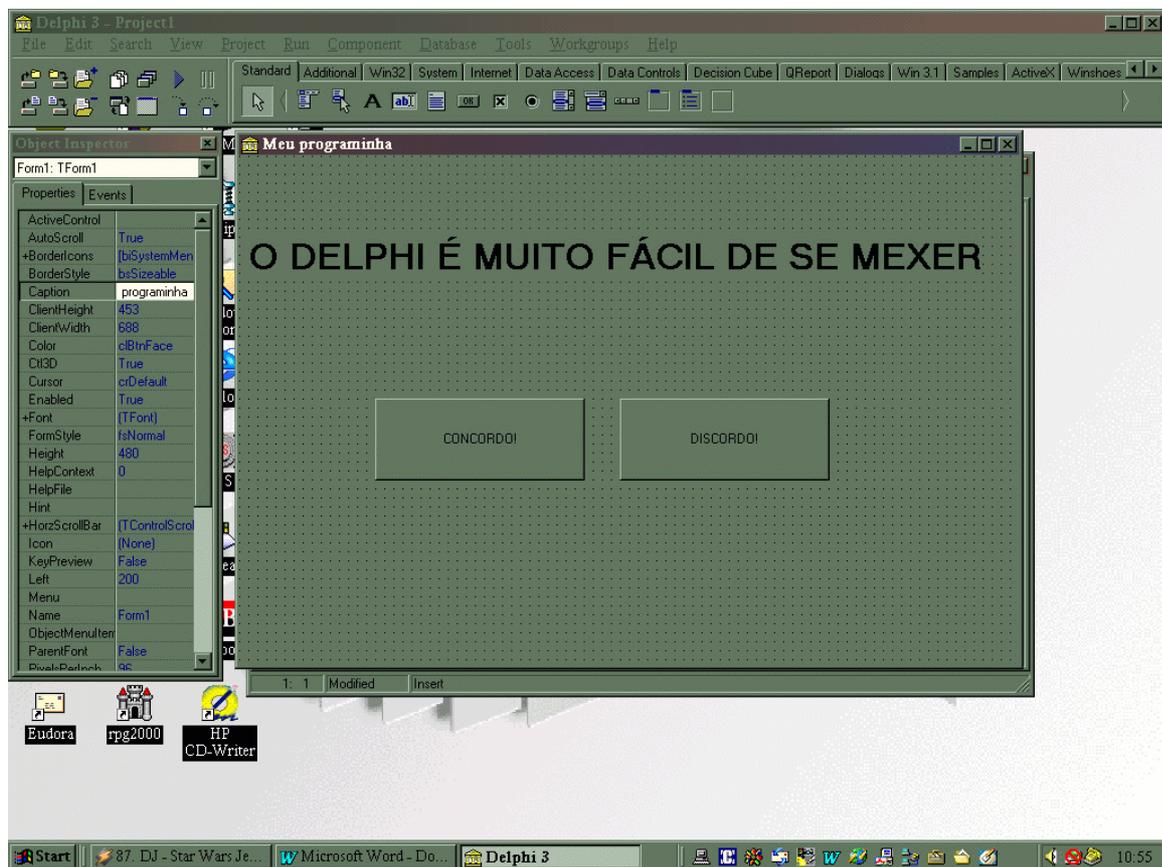
Por quê programar?

Uma vez um programador disse: "por quê me pagam para eu me divertir tanto?". A programação é essencial no mundo da segurança pois ela melhora o raciocínio e nos dá uma melhor visão lógica das coisas. Isso não significa necessariamente que você precisa ser bom na linguagem C. Alguns livros dizem que "hacker é o que sabe C, portanto aprenda na marra". Isso é uma mentira, conheço programadores ótimos em C que não sabem nem o que é endereço IP ou DNS. Aprenda uma linguagem de programação qualquer, dê preferência pelas mais fáceis como o Basic. Aos poucos vá avançando e tentando novas linguagens. Tente Perl (www.activeperl.com) que é uma boa opção. Você não precisa aprender para criar aqueles excelentes programas, o nosso objetivo aqui é que você entenda melhor como um programa funciona internamente, assim entendendo também como muitas das falhas podem ocorrem.

Linguagens orientadas a objeto

Antigamente precisava-se de muitas horas para construir a interface gráfica de um programa em código. As linguagens orientadas a objeto já possuem a criação da interface de um modo visual extremamente simples. A sua preocupação será então apenas as funções principais do programa já que os botões, caixas de textos e outros elementos gráficos são muito fáceis de se colocar. Os programas mais famosos que utilizam essas linguagens são o **Visual Basic** e o **Delphi**. Nós usaremos o Delphi nesse livro, pois acho-o de longe a melhor linguagem orientada a objeto e de quebra a mais fácil de se aprender.

Aprendendo a usar o Delphi

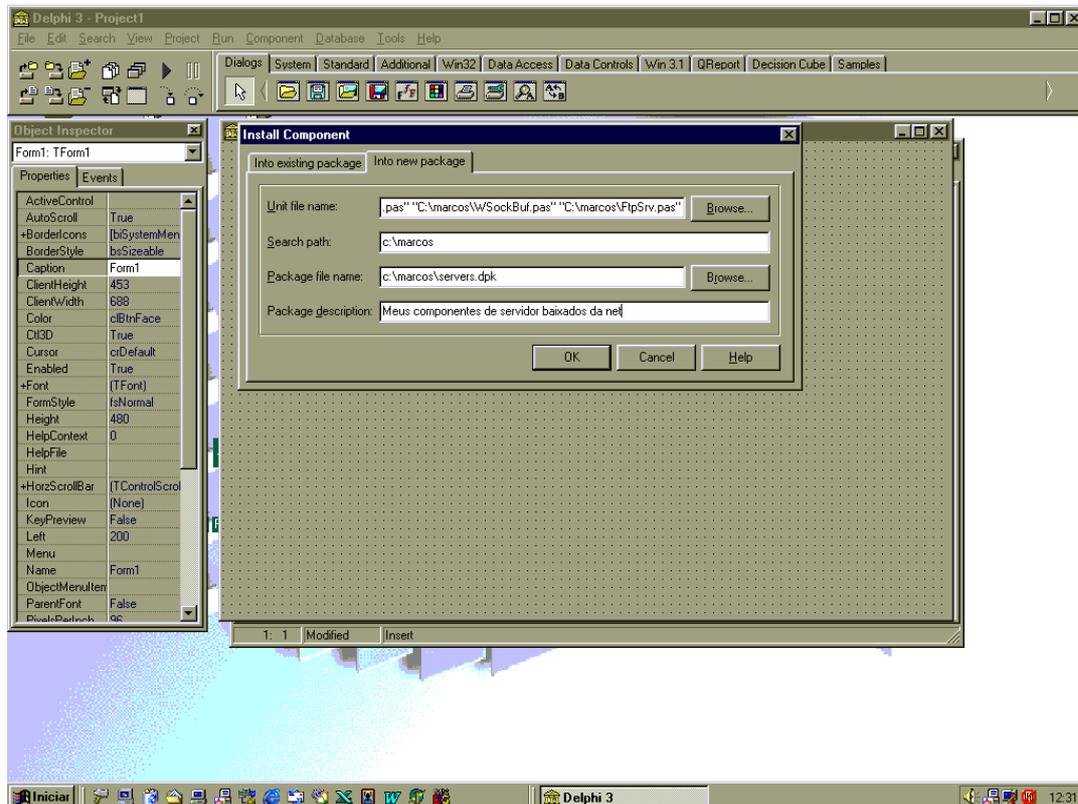
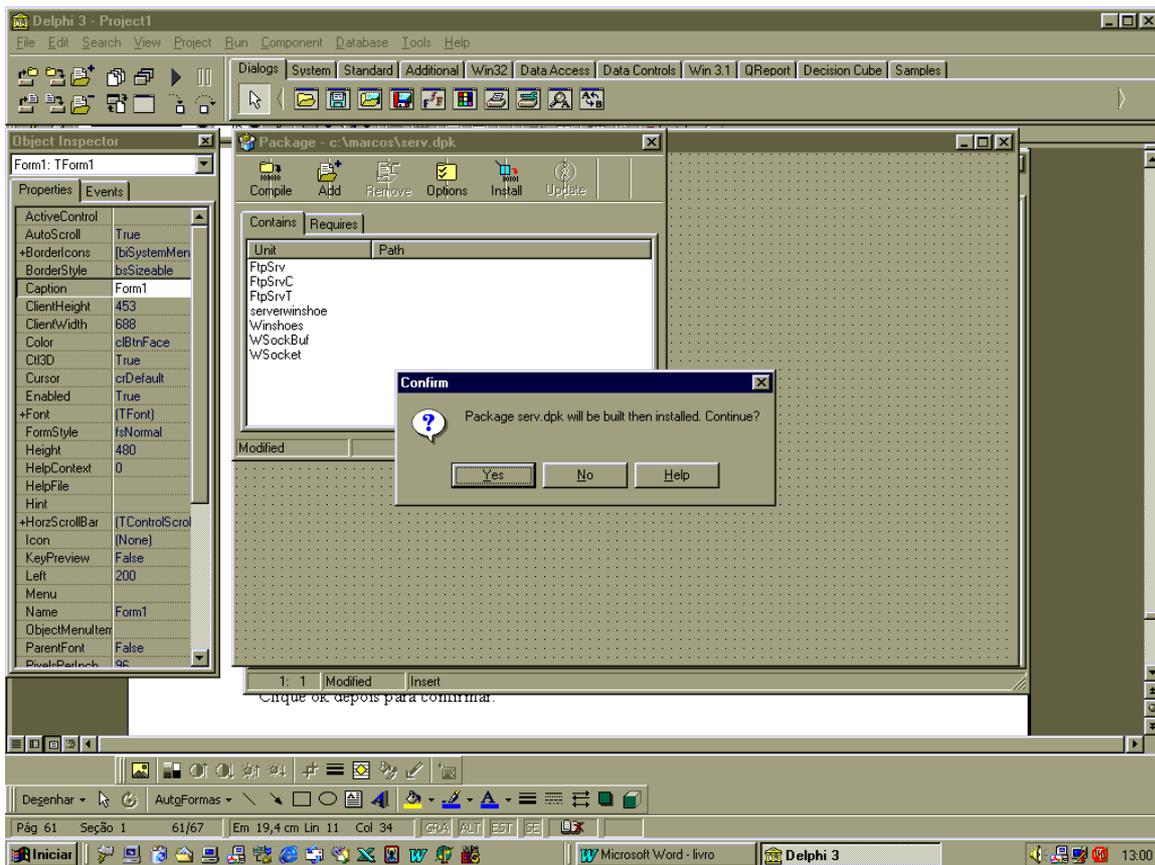
Não vou entrar muito em detalhes pois o nosso assunto principal não é programação. Utilizaremos a versão Cliente / Servidor do Delphi. É um programa simples de se mexer e quase totalmente visual. É só observar pela tela abaixo:

Observe que na parte superior existem pequenas ícones de ferramentas como botões, menus e caixas de texto. Se quiser colocar algum deles em seu programa, apenas selecione clicando-o e clique novamente no formulário (que é essa parte cinza com a frase: "O Delphi é muito fácil de se mexer"). Pronto. Se você apertar a tecla F9 seu "programa" irá rodar. Simples não?

A barra à esquerda têm a função de mostrar as propriedades de algum objeto colocado no formulário. Vamos supor que você queira mudar o título do programa (aquela frase que fica na barra superior de qualquer software). É só você selecionar o formulário dando um clique em cima dele , que o nome Form1 irá aparecer no gerenciador de objetos (conhecido anteriormente por barra à esquerda). Esse é o nome do nosso formulário, é dado pelo Delphi e pode ser modificado mas como estamos apenas dando uma leve noção continuaremos com esse nome mesmo. Agora observe algumas propriedades do formulário tais como: Color (cor), Font(fonte) e Caption. Essa última é a que nós queríamos. Selecione-a clicando no espaço à sua frente e escreva "Esse é o meu programa de teste". Aperte enter para confirmar. Prontinho. Se você aperter F9 de novo, a modificação já terá sido feita.

Todos os objetos funcionam assim: imagens, botões, gráficos, componentes de Internet, todos sem exceção possuem propriedades. E muitas em comum de um para o outro. É só fuçar um pouco (coisa que tenho certeza que se você comprou esse livro é porquê gosta) que logo aprende muita coisa.

Instalando os componentes necessários

Para que você possa construir os programas que serão explicados aqui, é necessário que você possua componentes (objetos) de Internet. Nem sempre o Delphi traz esses componentes, então preferi utilizar componentes extras. Aqui explicarei passo a passo aonde pegar esses componentes e como instalá-los sem maiores problemas.

- Visite o endereço **sunsite.icm.edu.pl/delphi/** , procure por ICS (Internet Component Suit) e pegue os componentes
- Execute o arquivo (ou descompacte-o se ele for no formato zip)
- Abra o Delphi
- Clique em Component e depois em Install Component. A seguinte tela irá aparecer:

Se você quiser instalar os componentes em um "pacote" (um conjunto de componentes) já existente, deixe selecionada a seção **Into existing package**. Se quiser criar um novo pacote, clique em **Into new package**, logo depois vá em Package file name e coloque o arquivo que você irá criar. Exemplo: c:\teste.dpk (todos os pacotes possuem extensão dpk). Procure onde está escrito **Unit file name**. Clique em **Browse** (o botão logo a frente). Vá no diretório em que você descompactou os componentes e selecione todos. Clique **ok** depois para confirmar. Vamos para a próxima tela.

Se você selecionou a opção de criar um novo pacote, o Delphi irá mostrar uma mensagem dizendo que o pacote será construído e instalado. Clique **Yes**. Caso a mensagem não apareça ou a opção de instalar em um pacote já existente foi selecionada, clique em Install ou Compile no quadrinho que apareceu (observe a figura acima). Pronto. Os componentes estão instalados. Na paleta de componentes (Dialogs, System, Standard...) vai aparecer mais um nome na barra de componentes: **Fpiette**.

Algoritmo

O que é um algoritmo? Nada mais é do que o projeto escrito de um programa. Algo como a receita de um bolo. Quando fazemos o bolo não colocamos manteiga, ovos e explicamos como o processo será feito (ex: bater duas vezes, levar ao forno por 15 minutos)? O programa também é assim. Um exemplozinho bobo de algoritmo segue na próxima página. É um programa que checa produtos para saber se têm poucas calorias ou não. Se tiverem, podem ser consumidos no SPA que comprou o programa. Se não, estão fora da lista.

Programa SPA;

DEFINIR Lugares = *Carrefour, Extra, Champion , Padaria do Mané*;

DEFINIR Preçomáximo = *50*;

PROCURAR Lugares por Mais Perto;

```
Com Mais Perto faça:
      Obtenha lista de Produtos;
      SE Produtos for maior que preçomáximo então:
            Desista;
            Volte pra casa;
      SENÃO
            Cheque Calorias;
            SE Calorias for menor que 100 então:
                  Compre;
            SENÃO
                  Continue procurando;
```

Difícil? Apenas aparentemente. É apenas pura lógica. Observe bem: Primeiro dissemos ao programa para definir os possíveis lugares para compra, que foram **Carrefour**, **Extra**, **Champion** e **Padaria do mané**. Depois definimos o preço máximo em 50 reais. Após feito isso, procuramos na variável **Lugares** (que contém 4 elementos) pelo mais perto. Obtendo o mais perto, o programa faz um pedido da **lista de produtos**. Se esses produtos forem mais caros que o preço máximo definido de **50** reais, então o programa desiste e volta pra casa. Se não, ou seja, se for mais barato que o preço máximo, hora de checar as calorias desses produtos. Se forem menores que **100**, compre. Se não, continue procurando.

Observe novamente as linhas do algoritmo acima e pense: por quê elas foram chegando para a direita? Isso se deve à **estrutura** de um algoritmo. Sempre que fazemos uma condição (como é o caso do **SE**) devemos colocar o código mais à direita. Exemplo:

```
SE Produtos for maior que preçomáximo então:
            Desista;
            Volte pra casa;
```

Nesse trecho do código, estamos respondendo à condição feita. Se escrevêssemos tudo em uma só linha ficaria mais fácil para entendermos:

SE Produtos **for maior que** preçomáximo **então** *Desista* **e** *Volte pra casa*;

Mas imagine se você tiver um algoritmo com 300 linhas? Isso seria confuso. A função de se colocar os comandos à direita (e na linha de baixo) de uma condição é somente **facilitar** quando tivermos um código grande e precisarmos encontrar algum trecho dentro dele. Se você ainda teve dúvidas, leia novamente e cuidadosamente o algoritmo. Pense logicamente. Será de grande ajuda para começarmos a meter a mão na massa de verdade.

Object Pascal

Object pascal é a linguagem de alto-nível utilizada pelo Delphi. Ela nada mais é do que um melhoramento do Turbo Pascal para Ms-Dos. É uma linguagem bem simples de se aprender e muito poderosa. Para acessar a janela do código, clique no formulário principal e aperte F12 ou simplesmente clique na janela branca que fica atrás desse formulário. Existem muitos e muitos comandos e diretivas para pascal. Vamos apenas ver os básicos que precisaremos no nosso exemplo de programa mais tarde.

Eventos : Todo objeto no Delphi (como o botão) têm propriedades. Isso nós vimos anteriormente quando mudamos o Caption do Formulário. Mas esses objetos também possuem mecanismos que os ligam ao código. Esses mecanismos se denominam *Eventos*. Se você colocar um botão no formulário e clicar duas vezes em cima dele, o Delphi o enviará para a tela de código usando o evento *OnButtonClick* (ou traduzindo, no clique do botão).

Assim é só você colocar algum comando. Quando o programa rodar (apertando F9) esse comando se executará assim que você clicar no botão. No **Object Inspector** à esquerda, está o modo correto de se acessar os eventos de um componente. É só clicar em **Events** e clicar duas vezes no evento desejado. Não se esqueça de selecionar antes o objeto dando um clique em cima dele. Achou difícil e complicado? Garanto que após o exemplo não achará mais.

Exemplo:

- Clique no componente **button** (botãozinho com um desenho escrito ok) e clique no formulário. O que você verá é isso:

- Clique duas vezes no botão que você colocou no formulário. Uma tela de código irá aparecer. Aperte espaço umas três vezes (para manter o código à direita, como foi mostrado em algoritmos) e digite **button1.color := clwhite;** Aperte F9 para rodar o programa. Clique no botão. Ahá, mudamos a propriedade de cor do botão para branco. Parabéns, seu primeiro programinha está pronto.

Criando os aplicativos

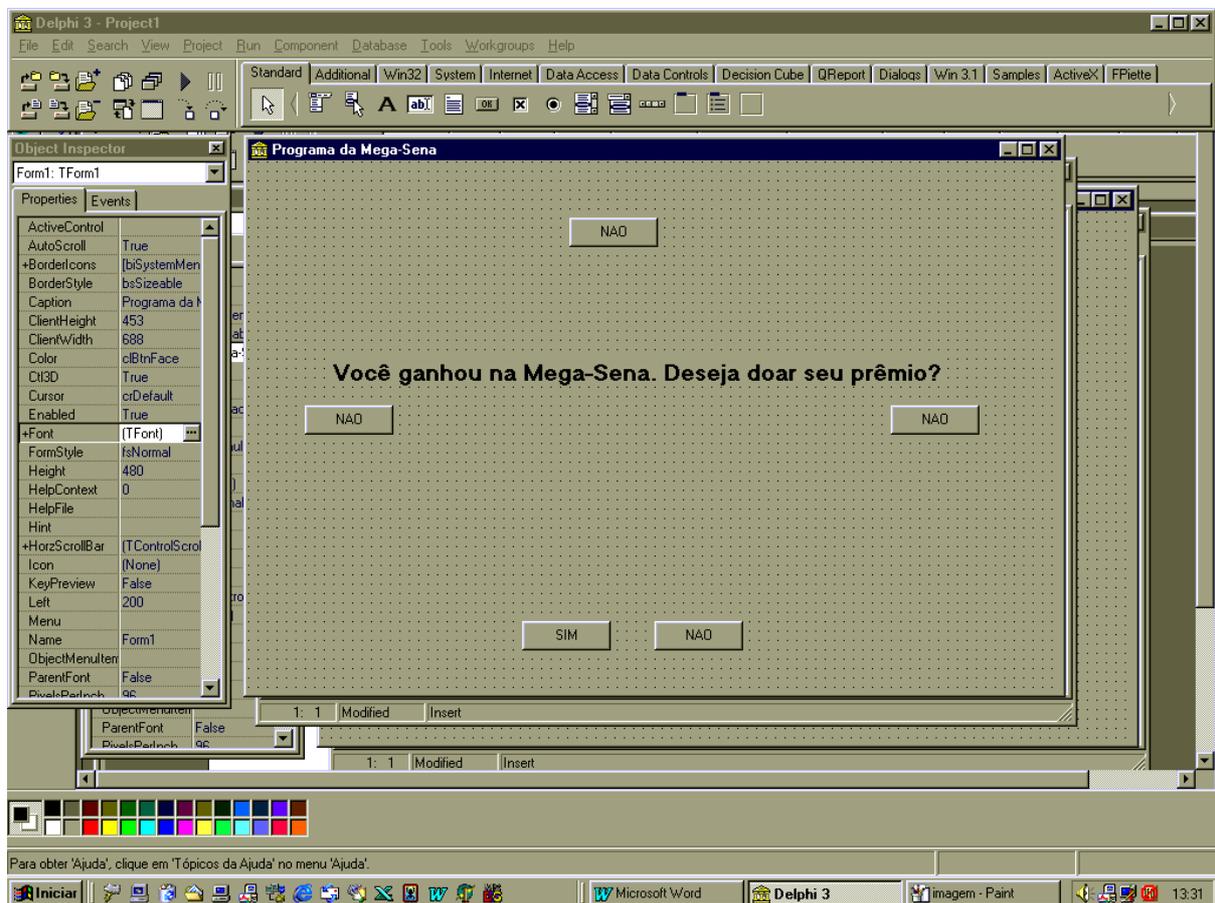
Visão geral

Vamos criar dois programas em Delphi para mostrar o poder dessa ferramenta. Nossos programas serão opostos: um trojan simples e um mini-firewall. Para ambos, utilizaremos apenas um componente: o **FtpServer**, que foi instalado na pasta de componentes Fpiette. É interessante notar que com um simples objeto (que funciona desde o primeiro Delphi à sua versão mais atual) podemos criar programas muito sofisticados. Claro que os que criaremos serão mais simples, apenas para exemplificar. Vamos criar primeiro o trojan.

Trojan simples

Nosso trojan consistirá em um mini-servidor FTP que ficará ativo na porta 2099 (se você tiver dúvidas sobre como se conectar a servidores FTP e o que são portas, dê uma lida no capítulo sobre protocolos). Criaremos um programa em que quando passamos o mouse em cima de um botão, esse some e aparece em outro local do formulário. É um daqueles programinhas bobos que vêm em revistas com o nome de " Inutilitários". Mas a nossa intenção é que a pessoa o utilize sem desconfiar que seu computador está aberto para o mundo. Vamos fazê-lo passo a passo.

- Coloque **cinco botões** no formulário do modo que demonstra a figura na página seguinte.
- Clique em cada um dos botões, vá em suas **propriedades** (mostradas no object inspector à esquerda) e mude o **caption** para "*NÃO*" (sem as aspas). Apenas no local que um botão está colado no outro, coloque o caption do botão da esquerda como "*SIM*".
- Selecione um **label** na barra de componentes (ilustrado com uma letra A) e coloque-o no formulário.
- Mude o caption do label para "**Você ganhou na mega-sena. Deseja doar seu prêmio?**"
- Vá nas propriedades do label, clique em **Font** (no espaço na frente da palavra Font). Clique no botãozinho com 3 pontinhos (...). Passe a fonte para negrito (bold) e coloque o tamanho 14. O tamanho deve ficar como o da figura.
- Agora, novamente clique em cada um dos botões, com exceção dos dois que estão juntos, vá em suas propriedades e mude o valor de **visible** (visível) de **true** para **false**. Ou seja, os botões ficarão invisíveis (na hora de rodar o programa).

O resultado do que fizemos será o mostrado a seguir.

Já sacaram do que se trata? O que faremos é incitar a pessoa a responder **NÃO** (quem iria querer doar um prêmio desses?), só que o botão irá "fugir" (na verdade o botão que o usuário passar o mouse em cima mudara seu status de visível para invisível e ao mesmo tempo outro dos botões escondidos ficará visível, dando a impressão de que o botão correu.). Bom, vamos para a segunda etapa do nosso trojan. Siga novamente esses passos:

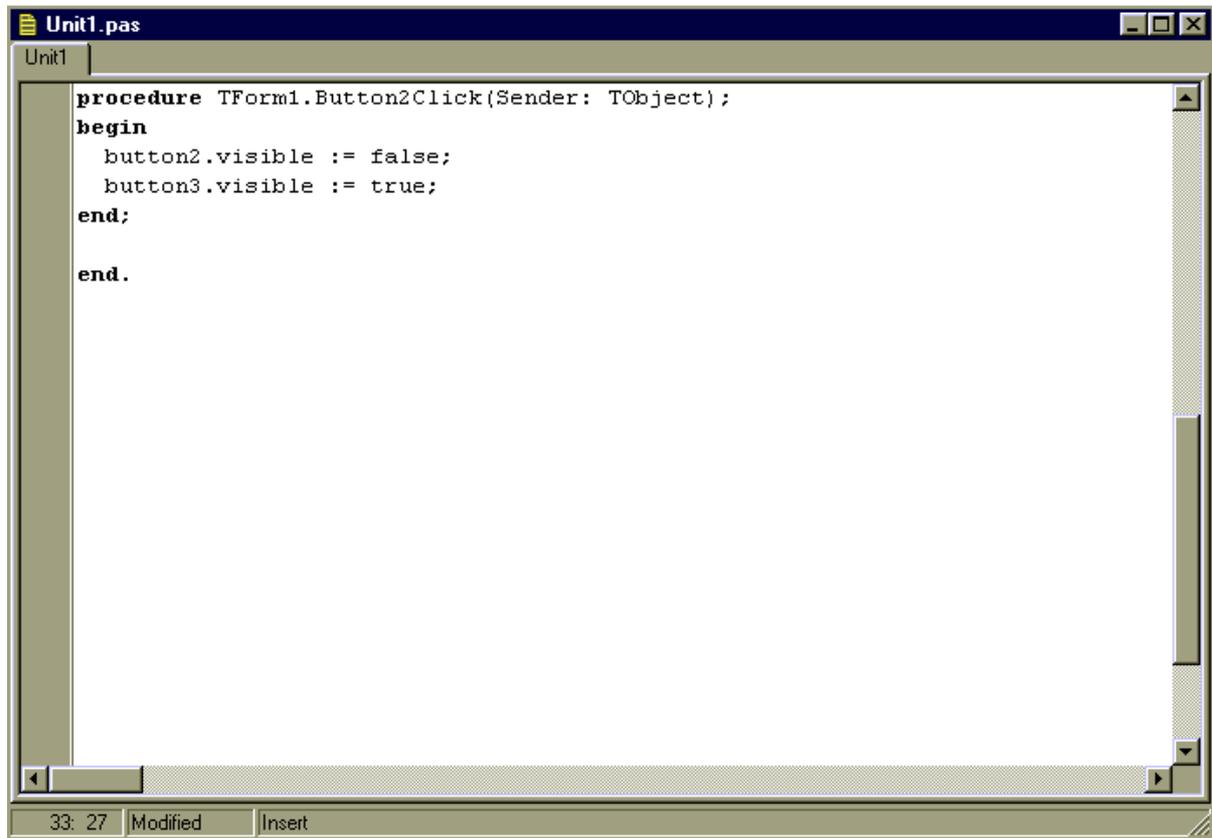
- Clique no primeiro dos botões em que está escrito NÃO para selecioná-lo. É o que está do lado do SIM.
- No **Object Inspector**, vá em Events e clique duas vezes na frente do evento OnMouseMove (é o evento que controla quando passamos o mouse em cima de alguma coisa).
- Logo que a tela de código aparecer, escreva as seguintes linhas (sempre estando no meio do **Begin** e do **End**):

Button2.visible := false;

Button3.visible := true;

- Tome cuidado com o nome dos botões. Para que você siga exatamente como está aqui é necessário que você tenha colocados os botões nessa ordem: Primeiro o SIM, depois o NÃO à sua direita, depois o NÃO que está a esquerda do formulário, o NÃO que está na parte superior e por último o NÃO à direita do formulário. Se não colocou nessa ordem, apague os botões (clicando em cima deles e apertando a tecla Delete) e coloque-os de

novo seguindo os passos na página anterior. Isso é importante para que os nomes desses botões coincidam com o exemplo.

O código será colocado como mostra a figura a seguir

Unit1.pas

Unit1

```
procedure TForm1.Button2Click(Sender: TObject);
begin
  button2.visible := false;
  button3.visible := true;
end;

end.
```

33: 27 | Modified | Insert

Vamos repetir esses procedimentos com todos os outros botões NÃO. Começando pelo botão à esquerda do formulário. Novamente selecione-o, vá em seus eventos (Events) e clique duas vezes em OnMouseMove. Coloque as seguintes linhas de código:

Button3.visible := false;

Button4.visible := true;

- Repita o procedimento com o botão NÃO no topo do formulário, inserindo o seguinte código:

Button4.visible := false;

Button5.visible := true;

- Calma aí gente, está quase acabando. Logo vou explicar o por quê dessas linhas de código. Agora o código do último botão NÃO à direita do formulário:

Button5.visible := false;

Button2.visible := true;

- Agora para variar um pouco, façamos o seguinte: clique no botão SIM uma vez, vá em seus eventos e clique duas vezes no evento **OnClick** (se quiser poupar trabalho, pode somente clicar duas vezes no botão SIM). Escreva o seguinte código:

Label1.Caption := "Você é muito bonzinho. Obrigado.";

Rode o programa e veja o resultado. Gostou? Pois é, o processo é muito simples: cada vez que se passa o mouse em cima de um botão (o qual podemos controlar usando o evento OnMouseMove) , esse botão vai mudar a sua propriedade **visible** para **false** (se visível é falso, o botão está o quê?) e mandar o próximo botão mudar a sua propriedade visible para true. E isso irá se repetir continuamente. Observe que no último código digitado, mandamos o botão de nome button2 ficar visível. Esse botão é o primeiro dos botões com o NÃO. Ou seja, nesse ponto, começamos tudo de novo.

Bom, isso foi apenas o que o nosso programa fingirá fazer. Agora que já construímos o seu falso código, vamos implementar o nosso servidor FTP.

- Na barra de elementos, selecione **FTPServer** e coloque-o no formulário.
- Clique no quadrinho do componente FTPServer, vá em suas propriedades e mude a porta (propriedade port) para 2099.
- Clique no formulário para selecioná-lo(Na parte vazia do formulário). Vá em seus eventos e clique duas vezes no evento **OnCreate**. Esse evento é chamado todas as vezes que o programa é iniciado. Para nós é perfeito, não queremos que nosso trojan esteja ativo com o início do programinha? Escreva o seguinte código (nunca se esquecendo que ele deve ficar entre o Begin e o End):

FTPServer1.Start;

Esse comando fará com o que o servidor FTP se ative e monitore a porta 2099. Se você for ao prompt do ms-dos e executar (com o programa rodando, é claro) **ftp 127.0.0.1 2099,** você se conectará ao trojan. Se quiser pode digitar a sintaxe do FTP direto pelo Windows, indo em Iniciar / Executar (sem necessidade de abrir o prompt).

Tudo está quase terminado agora. Só nos restou um problema: e se estivermos puxando algum arquivo e a pessoa fechar o programa? Nós iríamos ser desconectados. Para resolver esse problema, vamos "enganar" o usuário.

- Selecione o formulário clicando uma vez em cima dele. Nas propriedades, clique em duas vezes no símbolo "**+**" que está na frente da propriedade **BorderIcons**. Logo que a propriedade se expandir, clique na frente de **biSystemMenu** e selecione **false**. Isso fará com que aquele X que clicamos para fechar programas desapareça.
- Coloque um novo botão, e mude o caption para "*Fechar*". Clique duas vezes nele para acessar o evento **OnClick**. Agora coloque o seguinte código-fonte:

Form1.Visible := false;

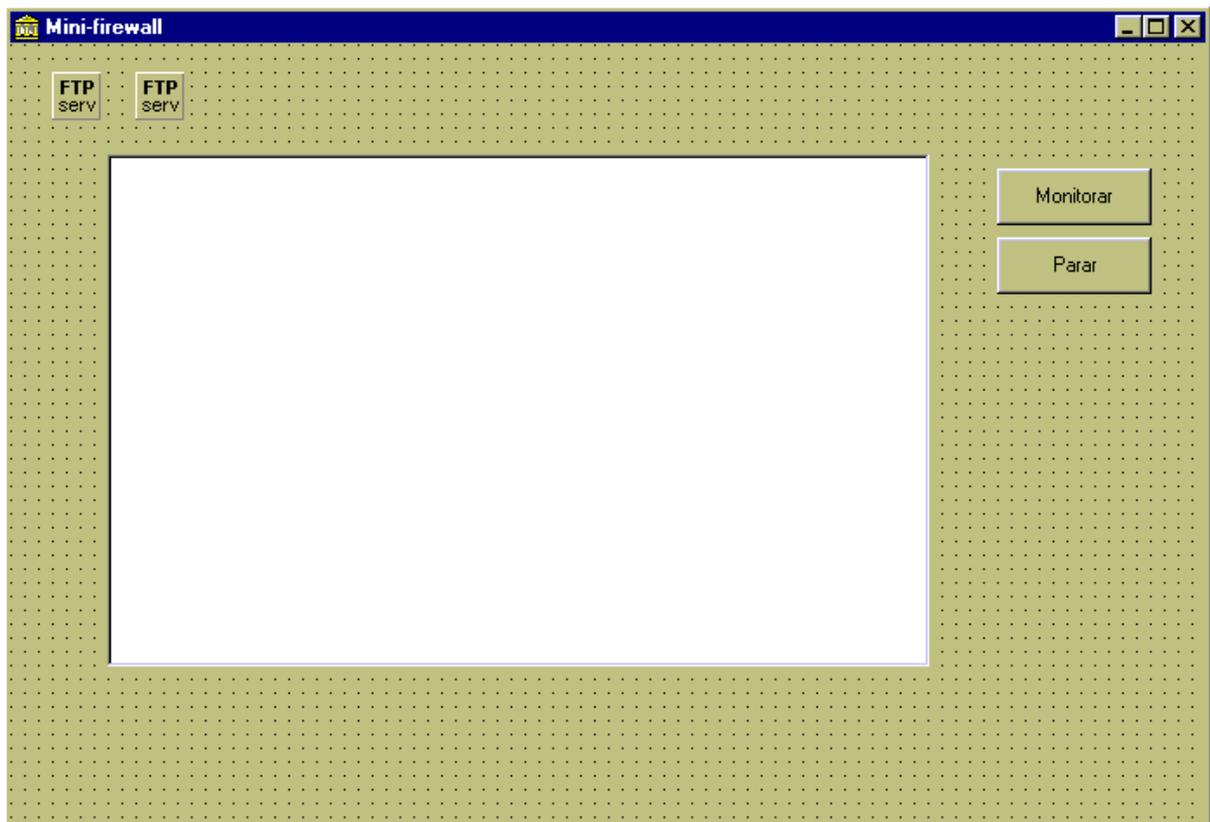
Como não existe mais aquele pequeno X para fechar a aplicação, o usuário clicará no botão Fechar. Mas na verdade, esse fechar apenas esconderá a aplicação. Ela ainda estará ativa e com o servidor FTP rodando bonitinho. Uma idéia de onde você pode colocar o botão fechar é mostrada na figura abaixo:

Nosso trojan está pronto. Ele é extremamente simples como deve ter dado para perceber, mas o meu interesse é que vocês tenham entendido como sua estrutura funciona ao invés de somente ficarem lendo toneladas de códigos-fonte inúteis (como alguns livros trazem). A partir desse ponto a criatividade a a imaginação ficam a cargo de vocês. Afinal, o programador nada mais é do que um artista. Renascentista.

Mini-firewall

A estrutura do mini-firewall será muito parecida com a do trojan. Na verdade, o nosso programa será um firewall de trojans. Manderemos que ele monitore duas portas TCP: a porta 12345 do trojan Netbus e a porta 1243 do trojan Subseven. Primeiramente, crie uma nova aplicação e adicione um campo **memo**, selecionando sua propriedade **enabled** para **false**. Agora seguiremos novamente passo a passo.

1. Adicione dois botões ao lado do campo memo e mude seus captions para **Monitorar** e **Parar**.
2. Coloque dois componentes **Ftpserv** no formulário.
3. Mude o nome (name) do primeiro componente para **Netbus** e sua porta (port) para **12345**.
4. Mude o nome do segundo componente para **SubSeven** e sua porta para **1243**.

Teremos mais ou menos isso:

Agora, selecione o componente ftpserv de nome Netbus, e vá em seu evento (event) *OnClientConnect*. Digite os seguintes comandos:

memo1.Lines.Add('O endereço IP '+ Client.GetPeerAddr +' tentou netbus');

```
netbus.DisconnectAll;
```

Não se esqueça do ponto e vírgula no fim das linhas. A primeira linha adiciona um texto no campo memo com o endereço IP do invasor. A segunda linha desconecta o indivíduo. Esse evento *onClientConnect* acontece no momento exato em que a pessoa estabelece uma conexão TCP com o seu computador.

Vamos repetir agora com o SubSeven. Selecione o componente, vá no evento *OnClientConnect* e digite essas linhas:

```
memo1.Lines.Add('O endereço IP '+ Client.GetPeerAddr +' tentou  Sub');
Subseven.DisconnectAll;
```

Nossos componentes já estão bem configurados. Agora só falta os botões. Clique duas vezes no botão de caption **Monitorar** e coloque:

```
Netbus.Start;
Subseven.Start;
```

Clique duas vezes (ou vá na propriedade OnButtonClick) no botão **Parar** e digite:

```
Netbus.Stop;
Subseven.Stop;
```

Como último passo, suba a barra de rolagem do código-fonte até encontrar a cláusula USES lá no início do texto. Será mais ou menos isso:

```
uses
  Windows, Messages, SysUtils, Classes, Graphics, Controls, Forms, Dialogs,
  StdCtrls, FtpSrv;
```

Agora inclua no fim da última palavra (que no caso do exemplo é ftpsrv mas não necessita obrigatoriamente que seja) a biblioteca **FtpSrvC**. Ficará assim:

```
uses
  Windows, Messages, SysUtils, Classes, Graphics, Controls, Forms, Dialogs,
  StdCtrls, FtpSrv, FtpSrvC;
```

Pronto. Rode o programa e curta seu mini-firewall. Tente conectar a ele usando o telnet.

19

Perguntas mais frequentes

O que é um FAQ (perguntas mais frequentes)?

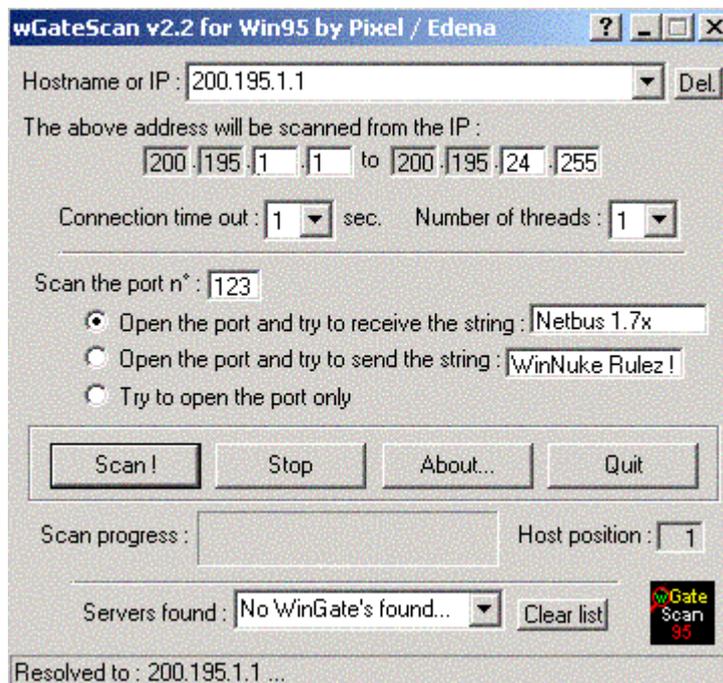
Quando tratamos de um assunto específico na Internet (uma página sobre os tipos de peixes existentes, por exemplo) , geralmente recebemos muitas perguntas e dúvidas de visitantes. Muitas dessas pessoas têm dúvidas em comum, por exemplo: qual é o maior peixe de água doce? Pegamos então esses perguntas e juntamos ela em um FAQ, ou perguntas mais frequentas, para que novos visitantes esclarecem essas dúvidas. No nosso caso não será diferente, esse capítulo é um Mini-FAQ com perguntas mais frequentes feitas a mim por usuários da Internet sobre o assunto.

Como descobrir o ip e derrubar pessoas em um bate-papo

Muitas pessoas me fizeram essa pergunta (algumas já haviam lido esse livro). A resposta é a seguinte: para derrubar alguém pode ser usado um ataque de denial of service. O IP que é o problema. Alguns tipos de chat, como o IRC mostram facilmente o IP de uma pessoa (a solução nesses casos seria usar um wingate para esconder o IP) e messengers como o ICQ também o mostram com facilidade (pois além do servidor você precisa estabelecer um contato direto, IP a IP, quando um arquivo é enviado por exemplo). Pegue por exemplo o programa **Trillian** (www.superdownloads.com.br). Ele pode servir como base para o Yahoo Messenger, o AOL Messenger, o MSN Messenger e o ICQ. E mostra o IP de qualquer pessoa, além de outras boas opções.

Agora, em bate-papos (me recuso a chamá-los de chat, são bate-papos mesmo) como UOL, TERRA ou qualquer outro baseado em servidor web é muito difícil descobrir o IP, pois o único endereço que você pode ver através de algum utilitário de rede (como netstat ou arp) é o do servidor da sala de bate-papo. Isso porquê nesse tipo de bate-papo a única intenção é conversar, não dá pra trocar informações diretas entre usuários (e obviamente saber seus endereços IP). A menos que você convença aquele cara chatíssimo a te enviar uma mensagem por ICQ, esqueça. Resumindo: quando alguém chegar em alguma sala do UOL dizendo “vou invadir todo mundo” ou coisas do tipo, ria um pouco da cara dele. Ou se ainda tiver dúvidas sobre a sua segurança, use um proxy. E caso encerrado.

Como posso diferenciar trojans de anti-trojans com um scanner?

Se você habilitar o anti-trojans e mandar scannear a subnet em que você está pela porta do Netbus (12345), o scanner mostrará que o seu computador está com a porta aberta. Mas como saber se essa porta é a de algum computador infectado ou é alguma armadilha, como um programa detector de invasões fingindo ser o trojan? A resposta é simples: Pela string. Ao usar um programa que conecte-se na porta especificada e verifique uma string você encontrará trojans facilmente e evitará as armadilhas. Exemplo:

O programa Wingate Scan permite que você o configure para mostrar portas com a string que você quiser, ótimo também para encontrar novos Wingates (string *wingate*>).

Eu posso usar o telnet para entrar em qualquer porta?

Sim e não. Pode usá-lo para entrar na porta que quiser, mas essa PRECISA possuir um serviço rodando ou não adiantará absolutamente nada. E nem todas as versões de telnet mostram conteúdos de portas. O telnet do Windows 95 , 98 e ME é uma porcaria. Experimente o **Port test**, uma espécie de telnet simples mas eficaz. Pegue-o em http://www.hackersclub.com/km/files/hfiles/ .

Por quê você colocou tão pouco de Linux / Unix no livro?

Uma ótima questão. Quem leu esse livro de cabo a rabo deve ter percebido que dei apenas uma breve introdução sobre o Linux e sobre o Windows, e apesar de a maioria dos exemplos de programas ser para Windows não me peguei realmente a nenhum sistema operacional. Veja o seguinte: parece uma contradição, disse bem lá no início que o Linux é melhor que o Windows, certo? Mas por quê citei programas para Windows?

Pressupõe-se que uma pessoa que tenha o Linux instalado em casa já tenha um conhecimento melhor do que uma que possui Windows. Então será muito mais fácil para ela ler as seções e procurar um programa similar ao que foi usado como exemplo. Nos sites

citados (inclusive no fim deste livro) existem excelentes ferramentas para Linux e Unix (entre outros sistemas, como Macintosh) que podem ser experimentadas sem maiores problemas. Resumindo: esse não é um livro sobre sistemas operacionais, é um livro sobre a segurança como um aspecto universal. Desejo que um usuário de BeOS por exemplo possa ler e mesmo que seu sistema não seja citado nem de longe, aproveite muito dos conhecimentos aqui citados.

Você me ajuda a invadir o sistema fulano de tal?

Por favor, não me façam esse tipo de pergunta. Não porquê eu me ache o sabichão, coisa que sei que não sou e nunca serei pois sou apenas mais um a aprender. Como disse no prefácio, informática, internet e segurança é a minha paixão. Aprendi a ler e escrever em um MSX. Comecei a conhecer sobre basic ali. Confesso que quando era mais novo realmente fiz muitas besteiras com o computador e só não me arrependo delas pois elas me trouxeram conhecimento e me fizeram amadurecer muito.

Bom, como dizem, àguas passadas não movem moinhos. Resumindo: não invado computadores , gosto apenas de divulgar o conhecimento que eu consegui obter e não quero causar prejuízos a ninguém. Tiro qualquer dúvida com o maior prazer, mas não me peçam pra fazer nada, por favor.

Se alguém tiver mais sugestões para o FAQ, me enviem que colocarei com o maior prazer.

20

Conhecendo mais do assunto

Sites de segurança versus sites de hackers

Para utilizar a Internet como um excelente veículo de aprendizado, você terá que ter algumas coisinhas em mente. A questão dos sites de segurança, por exemplo. Para saber novidades você não precisa visitar aquelas páginas escuras horríveis, com programas como o Winnuke para download, caveiras para todo lado e o texto "Invasão por IP". O interesse real está nos sites empresariais de segurança. Esses sim têm um conteúdo excelente, desde ferramentas, novos bugs descobertos e ótimos xploits. Sites como o *Technotronic (www.technotronic.com)* ou o *Security-focus* (www.security-focus.com) são apenas alguns dos incríveis sites que existem por aí. Visite-o periodicamente e esteja sempre procurando por novos scanners, ferramentas, firewalls, enfim, tome gosto pela coisa. As recompensas à longo prazo serão grandes: evitar dores de cabeça.

A importância do profissional de segurança

A menos que você seja um administrador que fica sentado o dia inteiro sem fazer absolutamente nada, não tenha medo de sugerir aos seus superiores a contratação de um especialista em segurança. Eles não irão lhe despedir, pelo contrário, verão que você está realmente interessado no bem da empresa. Explique que a àrea da segurança é muito grande e que todos os dias alguém deve visitar os sites especializados e procurar por atualizações e correção de bugs. E um especialista em segurança não é aquele que é PhD em ciências da computação. A informática muda muito rápido e as pessoas que fazem curso superior nessa àrea têm tanta coisa o que estudar que muitas vezes a segurança não é aprendida a fundo. Prefira os profissionais que fizeram cursos especiais (como cursos oficiais da Microsoft, da Conectiva ou da Cisco Systems).

Pense seriamente em contratar um hacker. Sendo uma pessoa que gosta do que faz, pode ter certeza que seu sistema estará bem seguro. Não seja levado por esse pensamento bobo de que é perigoso possuir um hacker trabalhando na empresa. Isso é uma bobagem pois ele é um funcionário como qualquer outro, com direito a promoções e ao olho da rua. Faça um contrato com ele em que ele se responsabilizará se algum ato ilícito acontecer por sua causa. É constrangedor, mas elimina o medo que os patrões têm.

Sites com matérias sobre o assunto

A grande maioria dos sites são em inglês. Afie bem o seu *vocabulary* pois são as melhores homepages do mundo.

www.blackhats.com

www.2600.com

www.security-focus.com

www.blackcode.com

www.undergroundnews.com

www.technotronic.com

www.cyberarmy.com

www.whitehats.com

www.cyberarmy.com

www.rootshell.com

www.securitysearch.net

www.hackernews.com

www.hackersclub.com

www.hackers.com

E alguns brasileiros:

www.securenet.com.br

www.txt.org **(site com textos ótimos)**

www.invasao.com.br

www.hacker.com.br

www.hackers.com.br

www.anti-trojans.cjb.net (website do programa Anti-Trojans feito pelo autor)

Filmes

A Rede

Hackers

Quebra de sigilo

Caçada virtual

Ameaça virtual

Piratas da informática

Jogos de guerra (war games)

Netforce

Jurassic Park (vale a pena ver uma "hacker" de saias)

Matrix (clássico)

Livros

Segurança Máxima – primeira e segunda edições

Hackers Expostos – primeira, segunda e terceira edições

Breaking into Windows systems (livro em inglês)